



VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA  
EKONOMICKÁ FAKULTA

KATEDRA APLIKOVANÉ INFORMATIKY

Inovace lokální sítě ve vzdělávací instituci  
Inovation of Local Network in an Educational Institution

Student:

Jan Kudela

Vedoucí bakalářské práce:

Ing. Petr Rozehnal, Ph.D.

Ostrava 2017

## Zadání bakalářské práce

Student:

**Jan Kudela**

Studijní program:

B6209 Systémové inženýrství a informatika

Studijní obor:

6209R017 Informatika v ekonomice

Téma:

Inovace lokální sítě ve vzdělávací instituci  
Inovation of Local Network in an Educational Institution

Jazyk vypracování:

čeština

Zásady pro vypracování:

1. Úvod
2. Teoretická východiska počítačových sítí
3. Analýza současného stavu počítačové sítě
4. Návrh inovací v síti a jejich implementace
5. Zhodnocení navrhovaného řešení a možnosti realizace
6. Závěr

Seznam použité literatury

Seznam zkratk

Prohlášení o využití výsledků bakalářské práce

Seznam příloh

Přílohy

Seznam doporučené odborné literatury:

SOSINSKY, Barrie A. *Mistrovství - počítačové sítě*. Brno: Computer Press, 2010.

ISBN 978-80-251-3363-7.

STANEK, William R. a Jiří HUF. *Microsoft Windows Server 2012: kapesní rádce administrátora*. Brno: Computer Press, 2015. ISBN 978-80-251-3817-5.

TRULOVE, James. *Sítě LAN: hardware, instalace a zapojení*. Praha: Grada, 2009.

ISBN 978-80-247-2098-2.

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Petr Rozehnal, Ph.D.**

Datum zadání: 18.11.2016

Datum odevzdání: 05.05.2017

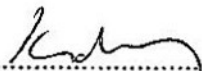
Ing. Petr Rozehnal, Ph.D.  
vedoucí katedry



prof. Dr. Ing. Zdeněk Zmeškal  
děkan fakulty

Prohlašuji, že jsem celou práci vypracoval samostatně.

V Ostravě dne 4.5.2017



.....

Jan Kudela

### **Poděkování**

Chtěl bych touto cestou vyjádřit poděkování Ing. Petru Rozehnalovi, Ph.D. za odbornou pomoc, cenné poznatky a trpělivost při psaní této bakalářské práce. Dále také ředitelce Základní školy v Hrabyni, Mgr. Monice Halfarové, za spolupráci. Poděkování za morální podporu také patří mé rodině a přítelkyni.

## Obsah

<b>1. ÚVOD .....</b>	<b>4</b>
<b>2. TEORETICKÁ VÝCHODISKA POČÍTAČOVÝCH SÍTÍ .....</b>	<b>5</b>
2.1. POČÍTAČOVÁ SÍŤ .....	5
2.2. DĚLENÍ SÍTÍ.....	5
2.3. AKTIVNÍ PRVKY SÍTĚ .....	8
2.4. SÍŤOVÉ STANDARDY .....	10
2.5. SÍŤOVÝ OPERAČNÍ SYSTÉM .....	13
2.6. VIRTUAL PRIVATE NETWORK.....	18
2.7. ZABEZPEČENÍ SÍTĚ .....	18
<b>3. ANALÝZA SOUČASNÉHO STAVU POČÍTAČOVÉ SÍTĚ.....</b>	<b>21</b>
3.1. INFORMACE O ŠKOLE .....	21
3.2. PŘEDSTAVA ŠKOLY O ZLEPŠENÍ .....	22
3.3. POPIS SOUČASNÉHO STAVU.....	22
3.4. SPECIFIKACE POŽADAVKŮ .....	25
<b>4. NÁVRH LOKÁLNÍ POČÍTAČOVÉ SÍTĚ.....</b>	<b>26</b>
4.1. NÁVRH SÍTĚ .....	26
4.2. VOLBA NOVÝCH PRVKŮ SÍTĚ .....	28
4.3. NASTAVENÍ AKTIVNÍCH PRVKŮ.....	30
4.4. PŘIPOJENÍ SERVERU .....	31
4.5. INSTALACE A KONFIGURACE ROLÍ SERVERU .....	31
4.6. ZABEZPEČENÍ SÍTĚ .....	41
4.7. VIRTUAL PRIVATE NETWORK.....	41
<b>5. ZHODNOCENÍ NAVRHOVANÉHO ŘEŠENÍ .....</b>	<b>43</b>
5.1. FINANČNÍ ANALÝZA NAVRHOVANÉHO ŘEŠENÍ .....	44
<b>6. ZÁVĚR.....</b>	<b>45</b>
<b>SEZNAM POUŽITÉ LITERATURY .....</b>	<b>46</b>
<b>SEZNAM ZKRATEK.....</b>	<b>47</b>
<b>PROHLÁŠENÍ O VYUŽITÍ VÝSLEDKŮ BAKALÁŘSKÉ PRÁCE</b>	

# 1. Úvod

Vývoj v oblasti informačních technologií jde závratně kupředu. Veškeré informace se digitalizují a na výkon výpočetní techniky jsou kladeny čím dál větší nároky. Pro většinu lidí je dnes nemyslitelné představit si běžný den bez počítače, a tudíž se dnes již s počítači setkáme téměř všude, například ve společnostech, domácnostech, knihovnách nebo školách.

Učitelé ve školách využívají výpočetní techniku denně mnoha způsoby, ať už pro přípravu látky na další dny, či jako podporu výuky. Vhodným využitím nepřeberného množství výukových programů se učení pro žáky rázem stává zábavnější. Žáci se také učí, jak pomocí internetu vyhledávat a získávat informace a pracují s nimi.

Počítačová síť, jejímž členem je také serverová stanice se síťovým operačním systémem, rozšiřuje možnosti každodenního využití počítačů. Učitelé například mohou látku zpracovávat u jakéhokoliv počítače a vždy mít ke svým dokumentům přístup, mohou s žáky sdílet materiály ve společných složkách, výukové programy se nemusí instalovat zvlášť na každou jednotlivou stanici a soubory přístupových práv a zabezpečení lze aplikovat hromadně na všechny počítače v síti.

Cílem této bakalářské práce je inovace stávající lokální sítě v základní škole. Tento může být rozdělen na dva podcíle. Prvním podcílem je vytvoření návrhu modernizace za použití serverové stanice se síťovým operačním systémem. Při návrhu bude brán zřetel na požadavky ze strany školy, bezpečnost, aby nedošlo k neoprávněnému vniknutí do sítě, a na jednoduchost údržby.

Druhým podcílem pak je samotná realizace řešení ve škole. Instalace serverové stanice, vytvoření uživatelských účtů, jejich rozdělení do skupin, přiřazení zásad těmto skupinám, dále připojení všech klientských počítačů do domény a připojení síťových složek k odpovídajícím účtům.

Nejprve budou definovány teoretické poznatky týkající se počítačových sítí a serverového operačního systému, dále bude následovat analýza současného stavu sítě a požadavků ze strany vedení školy a poté samotný návrh nové struktury počítačové sítě se začleněním serverové stanice.

## **2. Teoretická východiska počítačových sítí**

Hlavním tématem této kapitoly budou teoretická východiska související s návrhem a realizací počítačové sítě LAN. Zahrnuty budou poznatky přímo odpovídající obsahu této práce. Především se jedná o využití řešení pomocí síťového operačního systému, na kterém je tato práce založena.

### **2.1. Počítačová síť**

Počítačová síť představuje obecně systém vzájemně propojených počítačů, terminálů, a dalších zařízení, komunikujících prostřednictvím komunikačního subsystému sítě, přenosových médií a aktivních prvků (Kállay a Peniak, 2003). Sosinky (2010) dodává, že skupina prvků může být považována za síť, pokud obsahuje následující atributy: propojovací software, síťové systémy a síťové prvky (jako například přepínače, fyzická přenosová média a adresní systém). Každá počítačová síť se pak skládá z těchto komponent:

- Propojené systémy
- Propojovací software
- Síťový hardware
- Fyzická přenosová média
- Adresní systém pro všechny výše uvedené komponenty

### **2.2. Dělení sítí**

Taxonomie neboli klasifikace je rozdělování počítačových sítí podle nejrůznějších kritérií. Tato kritéria nemusí být přesně vymezena a jejich hranice nemusí být jednoznačně dané. S dalším vývojem technologií, s časem nebo i s potřebami uživatelů se tyto hranice v čase mění (Peterka, 2012).

#### **2.2.1. Dělení podle topologie**

První variantou taxonomie počítačových sítí je dělení dle topologie. Sosinsky (2010) uvádí, že jde o rozložení nebo seřazení síťových prvků, a to jak zařízení, tak i jejich propojení. Jelikož vše se síťovou adresou je považováno za síťový prvek, lze označit jako logický či virtuální síťový prvek také software a je nutné jej zahrnout do popisu topologie.



Dále Sosinsky (2010) dodává, že fyzická topologie se zabývá také vztahy mezi prvky tvořícími síť. Logické topologie naopak mapují trasu, kterou musí pakety absolvovat na cestě mezi uzly. Logickou topologii je možné sestavit, pouze pokud jsou uzly v síti dostupné prostřednictvím protokolů pro výměnu dat.

Trulove (2009, s. 48) uvádí, že „*tři základní síťové topologie se jmenují sběrnice, kruh a hvězda. Některé sítě, například Ethernet, tyto topologie kombinují. Každá z topologií má své výhody a nevýhody.*“

### **Topologie sběrnice**

Sběrnice je velmi běžným přenosovým médiem. Spojuje dva nebo více síťových uzlů zvaných koncové body. Tyto koncové body označují takové uzly, které mají klíčovou vlastnost pro síťovou komunikaci: schopnost být adresovány. Síťová karta počítače může získat adresu, a je tedy koncovým bodem čili uzlem sítě, a stejně tak směrovač. Z hlediska základního principu adresovatelnosti mohou být koncovými body sběrnice také jednotlivé porty směrovače či prepínače (Sosinsky, 2010).

### **Topologie kruhu**

Kruhová topologie postupně připojuje jednu stanici ke druhé, až nakonec poslední stanici připojí zpět k první a vznikne kruh. Data chodí v kruhu od jednoho zařízení k druhému, dokud nedojdou až ke svému příjemci. Digitální signál se obvykle na každém uzlu obnovuje a síť většinou používá nějaký token, který řídí vysílání a brání ucpání sítě. Příkladem kruhové topologie jsou Token Ring a FDDI (Fiber Distributed Data Interface) (Trulove, 2009).

### **Topologie hvězdy**

Hvězda je velmi často používanou síťovou topologií. V hvězdicové síti se jednotlivá bodová spojení odvětvují z jediného centrálního uzlu. Tomuto uspořádání se někdy také říká rozbočení. Všechna data prochází v této síti nutně centrálním uzlem. Nejsnáze může být hvězdicová síť vytvořena s pomocí patch panelu, nebo se může naopak jednat o aktivní spojení s přenosem dat, korekcí chyb a zesilovačem signálu. Sítě s topologií hvězdy se mohou stavět i tak, že centrální rozbočovač propojuje dvě nebo více hvězdicových sítí dohromady. To je případ jak rozšířené, tak distribuované hvězdicové topologie (Sosinsky, 2010).

Trulove (2009) dodává, že v moderních sítích ji zastupuje velice oblíbený Ethernet se svými rozbočovači a prepínači.

### 2.2.2. Dělení dle rozlehlosti

Další možností klasifikace počítačové sítě je dle rozlehlosti. Kállay a Peniak (2003) uvádí tři základní kategorie:

- **LAN** (Local Area Network) jsou malé lokální sítě. Jejich dosah je obvykle maximálně 10 km (nejčastěji budova, hala, továrna apod.).
- **MAN** (Metropolitan Area Network) jsou sítě na území města, tedy řádově desítky km, skládající se obvykle ze vzdálených sítí LAN.
- **WAN** (Wide Area Network) jsou sítě dosahující největších vzdáleností. Pokrývají území států i celých kontinentů.

Sosinsky (2010) dále dodává další dvě kategorie a těmi jsou sítě:

- **PAN** (Personal Area Network), které jsou z hlediska uspořádání nejmenšími sítěmi. Jejich dosah je asi 10 metrů. Označení PAN se obvykle vztahuje na skupinu periferních zařízení připojených k jedinému počítačovému systému. Typickým příkladem PAN je technologie Bluetooth.
- **CAN** (Campus Area Network) jsou univerzitní sítě pokrývající skupinu budov.

### 2.2.3. Dělení dle architektury

Dle použité architektury a zpracování dat uvnitř sítě, je lze rozdělit na několik druhů. Nejpoužívanějšími architekturami jsou Peer-to-Peer (P2P) a Klient-Server.

- **Peer-to-Peer**

Sítě typu peer-to-peer (P2P) jsou první ze sady síťových architektur. Hlavním rozlišujícím faktorem, který rozhoduje, zda síť má architekturu P2P nebo jinou, je účast všech uzlů ve vzájemné interakci na síti a zpracování dat jako prakticky zcela rovných partnerů, uzly mohou hrát zároveň roli klienta i serveru. Mezi jednotlivými uzly jsou přitom přímá spojení. Taková síť nemá žádné centrální řízení. Hlavní výhodou P2P sítí je možnost sdílet distribuované prostředky. Není nutná zbytečná duplikace zdrojů a celkové náklady jsou nižší. Příkladem takové sítě je pracovní skupina v prostředí Microsoft Windows, skládající se z tuctu nebo méně členů.

Výhodou této architektury je zejména fakt, že pro správu sítě nejsou třeba žádné velké znalosti a jedná se o velmi levné řešení, jelikož není nutné kupovat server ani žádné síťové operační systémy.

Nevýhodou může být, že při větším počtu počítačů je velmi obtížné udržet přehled o datech. Data jsou málo chráněna proti zneužití. Konfigurace přístupových práv je u peer-to-peer jednoduchá (a méně bezpečná), navíc se musí aplikovat na všech stanicích, což bývá neuskutečnitelné (Horák, 2011).

- **Klient-Server**

Sítě fungující podle vzorce klient-server používají dvouvrstvou architekturu, ve které zpracování dat provádí serverový systém a poskytuje je pak klientskému systému nebo systémům. Architektura klient-server se v současnosti uplatňuje jako nejrozšířenější forma síťové distribuce výpočetní síly a velmi často ji najdeme v síťových aplikacích, jako jsou databáze, webové stránky, elektronická pošta a další technologie.

V technologii klient-server je nutné, aby na straně serveru běžel serverový software, zatímco u klienta se očekává klientský softwarový protikus. Jedinou podmínkou úspěchu je schopnost vzájemné komunikace mezi klientem a serverem prostřednictvím odpovídajících protokolů. Pro správnou funkci aplikace s architekturou klient-server musí být definován protokol, jehož prostřednictvím klient žádá server o službu, a další protokol, s jehož pomocí server poskytuje data nebo přenáší zpět data zpracovaná, původně zaslaná klientem (Sosinsky, 2010).

Výhodou je vysoká bezpečnost dat, přehlednost a snadná konfigurovatelnost. Naopak nevýhody spočívají v nákladech na nákup serveru a síťového operačního systému a v nutnosti mít kvalifikovaného pracovníka, který bude umět obsluhovat síťový operační systém (Horák, 2011).

## **2.3. Aktivní prvky sítě**

V sítích se musí používat propojovací zařízení, která vytvářejí síťové okruhy. Mezi ně patří rozbočovače, mosty, prepínače, směrovače a brány. Existují dva základní typy sítí: síť s přepínáním okruhů a síť s přepínáním paketů.

Sosinsky (2010, s. 197) říká, že „*síť s přepínáním okruhů je definována fyzickým nebo virtuálním okruhem (spojením) mezi dvěma koncovými body a vyznačuje se jistou šířkou pásma. Okruh musí být definován po celou dobu předávání zpráv v síti. Zařízení provádějící funkci*

*přepínání může být překonfigurováno, okruhy se tedy mohou v čase měnit a celá síť může být upravena dle potřeby. “*

Síť s přepínáním okruhů má oproti přepínání paketů své výhody. V síti s přepínanými okruhy je vždy celá zpráva odeslaná pomocí toho stejného okruhu, což může být rychlejší než zasílání kusu zprávy různými cestami. Když zpráva dorazí do cíle, děje se tak ve správném pořadí a proud dat nemusí být znovu sestavován

Dále Sosinsky (2010, s. 198) uvádí, že *„síť s přepínáním paketů je založena na jiném principu. Za každých okolností se hledá nejlepší dostupná trasa. Jednotlivé pakety jsou v tomto případě předávány od zdroje k cíli nejlepším možným spojením, o kterém přepínací zařízení ví. Tento druh přenosu je určen pro nenapravitelně nespolehlivé sítě, v nichž každé spojení může být jen přechodné.“*

Výhodou přepínání paketů může být lepší využití kapacity sítě, protože provoz může být rozložen mezi více spojení. Náklady nutné pro sestavení příchozích paketů do správného pořadí a malá ztráta výkonu vyvažuje lepší využití sítě a vyšší tolerance vůči chybám (Sosinsky, 2010).

### **2.3.1. Rozbočovač**

Rozbočovač je nezbytným prvkem v sítích s hvězdicovou topologií. Jeho základní funkcí je rozbočování signálu neboli větvení sítě (Horák, 2011).

Sosinsky (2010) dodává, že jde o velmi prosté zařízení, které propojuje síťové uzly ve stejném segmentu, obvykle prostřednictvím kabelu s kroucenou dvoulinkou nebo s optickými vlákny. V dnešní době jsou rozbočovače překonány a nahradily je přepínače.

### **2.3.2. Most**

Most je zařízením starším, jehož hlavním úkolem je oddělení síťových segmentů. Most je inteligentním prvkem, který se zajímá o přenášená data. Hlavními dvěma funkcemi je filtrace paketů a propojení dvou sítí různých standardů (Horák, 2011).

### **2.3.3. Přepínač**

Přepínač představuje aktivní zařízení, které spojuje dvě sítě na jedné nebo více vrstvách síťového modelu OSI. Označení přepínač se používá pro širokou škálu prvků, tudíž neexistuje žádná pevná definice přepínače (Sosinsky, 2010).

Přepínače dnes nahradily rozbočovače v centru všech sítí s hvězdicovou topologií. Při komunikaci vytvoří mezi oběma komunikujícími stanicemi spojení oddělené od stanic ostatních. Stanice tedy nejsou zahlcovány cizími pakety, nedochází ke zpomalování sítě a výměna dat mezi koncovými stanicemi probíhá maximální rychlostí (Horák, 2011).

#### **2.3.4. Směrovač**

Směrovač je zatím nejinteligentnějším aktivním prvkem. Pracuje na úrovni síťové vrstvy ISO/OSI. Shromažďuje informace o připojených sítích a pak vybírá nejvýhodnější cestu pro posílání paketů. Má v sobě zabudovanou filtraci paketů, kterou doplňuje o inteligentní směrování (Horák, 2011).

Směrování v malých sítích není aplikací náročnou na zpracování procesorem, proto se často jako směrovače používají starší osobní počítače. Díky nízké ceně jsou jako směrovače velmi populární linuxové servery (Sosinsky, 2010).

Směrovače využívají logických adres spojovaných sítí a uzlů pro logické členění sítě a budování směrovacích tabulek. Směrovač na základě vybudované směrovací tabulky směruje jednotlivé pakety podle jejich cílové síťové adresy. Rozlišujeme směrování přímé, kdy je cílová logická síť přímo na určitém portu směrovače a nepřímé, pomocí mezilehlého směrovače. K funkcím směrovače patří:

- logická adresace sítí a uzlů intersítě,
- údržba směrovacích tabulek a komunikace ve směrovači sítě,
- odebrání a přidávání záhlaví linkové vrstvy u paketů,
- výběr optimální cesty pro paket s cílovou adresou,
- zpracování paketů různé délky pro síť (Kállay a Peniak, 2003).

#### **2.4. Síťové standardy**

Jelikož se jednotlivé síťové prvky dají různě kombinovat, byly přijaty normy – standardy, které definují základní požadavky na technické provedení sítí. Normalizaci provádí organizace IEEE (Institute of Electrical and Electronics Engineers), tudíž jednotlivé normy nesou její označení. Pro síť LAN jsou nejdůležitější tyto standardy:

- **IEEE 802.3** – Standardy sítě Ethernet,
- **IEEE 802.4** – Sběrníkové sítě s metodou přístupu token,

- **IEEE 802.5** – Kruhové síť s metodou přístupu token,
- **IEEE 802.11** – Pro bezdrátové síť.

Z praktického hlediska jsou nejdůležitější tyto standardem definované vlastnosti:

- přístupová metoda,
- topologie sítě,
- typ kabelu, jeho délka, způsob připojení stanic (konektor),
- rychlost přenosu dat (Horák, 2011).

#### 2.4.1. Ethernet a jeho členění

Síť Ethernet lze rozčlenit do několika kategorií podle nejvyšší podporované rychlosti:

- **10BASE-5** – nejstarší, dnes nepoužívaný Ethernet s maximální přenosovou rychlostí 10 Mb/s. Základem byl tlustý koaxiální kabel a sběrníková topologie (Horák, 2011).
- **Fast Ethernet 100BASE-T** – technologie 100 Base T navazuje na vlastnosti a koncepci osvědčené sítě Ethernet 10 Base T. Podporována je podobná topologie sítě, typ kabeláže, použitá přístupová metoda a typ rámců MAC. Rychlost vzrostla na 100 Mb/s.
- **Gigabitový Ethernet 1000BASE-T** – standardizován byl v roce 1988. Gigabitový Ethernet plní kritéria kompatibility, jelikož podporuje stejný formát rámce, kolizní metodu CSMA/CD a použití hvězdicové topologie. Povoleno je použití opakovačů, přepínačů a jsou podporovány i existující typy přenosových médií. Přenosová rychlost činí již 1 Gb/s (Kállay a Peniak, 2003).
- **10 GB Ethernet 10GBASE-T** – norma nejrychlejšího Ethernetu vyvíjena nejen pro síť LAN, ale je také použitelná pro síť MAN a WAN. V roce 2003 byl standardizován pro optické kabely a v roce 2006 pro kroucenou dvoulinku.

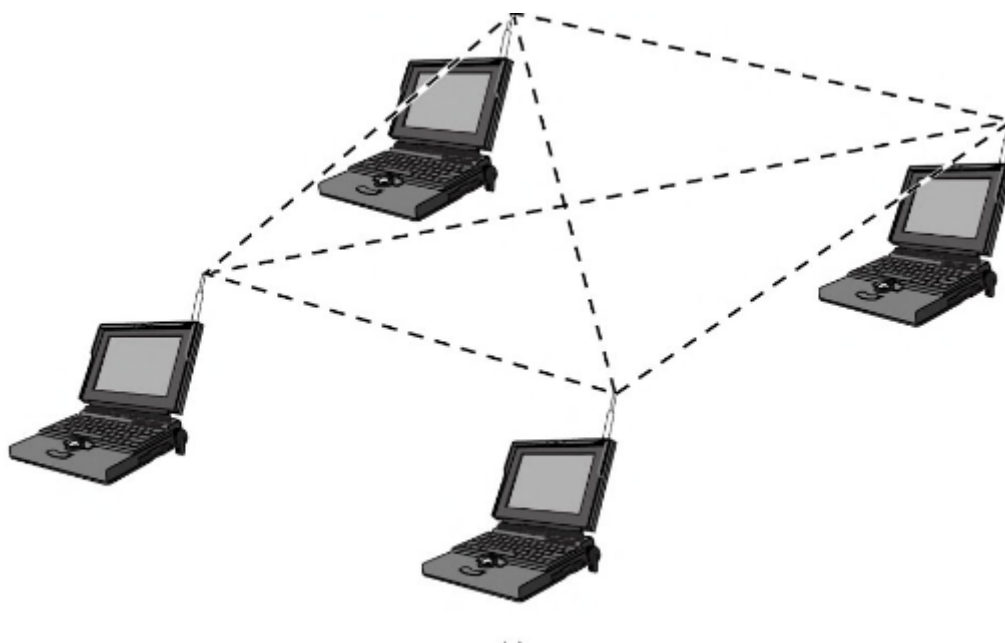
### 2.4.2. Bezdrátové sítě LAN

V bezdrátových sítích existují dva typy architektur: ad hoc režim a infrastrukturní režim. Běžně používané standardy jsou všechny založené na komunikačních linkách vytvořených s pomocí rádiových frekvencí ve veřejných pásmech 2,4 GHz nebo 5 GHz. Tato pásma jsou vybrána proto, že přístup pro veřejnost je zcela volný a jsou navíc schopna pojmout ad hoc síťové spoje (Sosinsky, 2010).

Bezdrátové sítě používají dva druhy architektur:

- **Ad hoc síť**

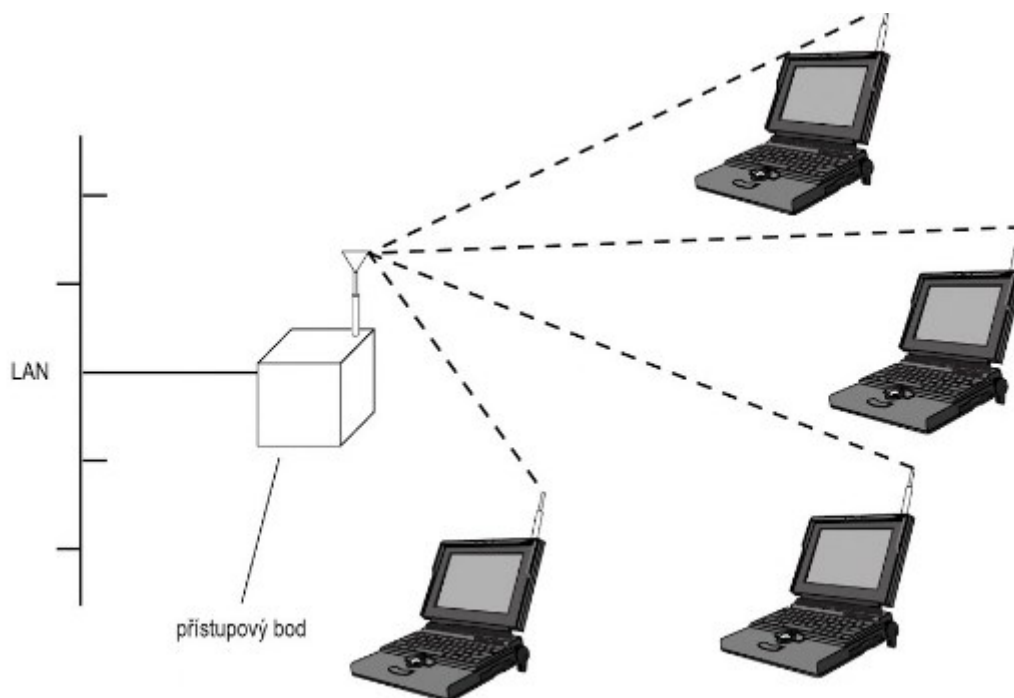
Tato architektura umožňuje komunikaci libovolných dvou nebo více stanic s bezdrátovými kartami. Jedna bezdrátová karta se dočasně (ad hoc) ujme velení a řídí vysílání všech stanic. Hlavní nevýhodou této architektury je absence hlavního spojovacího bodu mezi bezdrátovou a klasickou sítí a chybí též jeden centrální bod, který by mohl řídit výměnu informací (Trulove, 2009).



Obrázek 2.1: Síť Ad Hoc. Zdroj: Trulove 2009.

- **Infrastrukturní síť**

V tomto režimu se o řízení provozu sítě stará zařízení označované jako přístupový bod neboli access point (AP). Bezdrátové sítě typu klient-server jsou obvykle rychlejší a spolehlivější (Trulove, 2009).



Obrázek 2.2: Infrastrukturní síť. Zdroj: Trulove 2009.

## 2.5. Síťový operační systém

Síťový operační systém je operační systém, který je optimalizován pro poskytování síťových služeb jiným systémům v síti. Každý síťový operační systém musí poskytovat podporu hardwaru, spouštět protokoly a služby a poskytovat tyto služby nebo aplikace klientským systémům. Kromě těchto základních služeb může síťový operační systém nabídnout nástroje pro správu, jmenné a adresářové služby, souborové a tiskové služby, webové služby, zálohování, zabezpečení a síťové směrování, stejně jako by měl sloužit jako operační systém, na němž lze nainstalovat a spouštět síťové aplikace (Sosinsky, 2010).

Mezi dnes používané nejpopulárnější síťové operační systémy patří:

- Unix
- Linux
- Solaris
- Novell NetWare a Open Enterprise Server
- Windows Server



### 2.5.1. Windows Server 2012

Microsoft Windows Server 2012 je výkonný, univerzální a funkcemi nabitý serverový operační systém založený na funkcích, které byly poprvé použity u systému Windows Server 2008 R2. Díky společnému vývoji nabízí systémy Windows Server 2012 a Windows 8 totožné funkce, jež vychází ze stejného základního kódu a přesahují do četných oblastí, například do oblasti správy, zabezpečení, sítí a úložišť (Stanek, 2015).

Při instalaci Windows Serveru 2012 si můžeme vybrat ze tří typů:

- **Instalace serveru s grafickým uživatelským rozhraním** – tato možnost zajistí plnou funkcionalitu serveru a je často označována jako kompletní instalace. Správa se provádí pomocí uživatelského rozhraní.
- **Instalace jádra serveru (Server Core)** – tato možnost poskytuje minimalistickou aplikaci, která nabízí pevnou sadu rolí, avšak neobsahuje grafické prostředí serveru, konzoli Microsoft Management Console ani součást Možnosti práce s počítačem.
- **Instalace serveru s minimalistickým rozhraním** – poslední možnost instalace, představující střední cestu. Dochází při ní k instalaci kompletního serveru a následnému odstranění grafického prostředí serveru (Stanek, 2015).

### 2.5.2. Funkce a role systému Windows Server 2012

Windows Server nabízí velké množství rolí. Základní rolí je AD DS (Active Directory Domain Services), společně s ní se instaluje role Server DNS. Všechny další role je možné kdykoliv přidat a odebrat. Mezi další role patří:

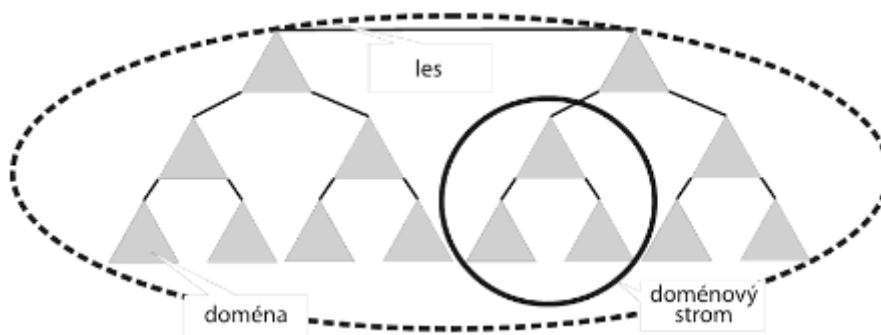
- DHCP Server,
- Souborová služba a služba úložiště,
- Tiskové a dokumentové služby,
- Vzdálený přístup,
- Webový server.

### a) Active Directory Domain Services

Služba AD DS je rozšiřitelnou a škálovatelnou adresářovou službou, která umožňuje efektivně spravovat síťové zdroje. Již od verze Windows 2000 představuje tato služba srdce domén s operačním systémem Microsoft Windows. Má na ni vliv prakticky každý prováděný úkon správy. Technologie Active Directory se zakládá na standartních internetových protokolech a je navržena tak, aby pomohla jasně definovat síťovou strukturu (Stanek, 2015).

Active Directory poskytuje síťovým komponentám logickou i fyzickou strukturu. Logická struktura napomáhá při organizaci adresářových objektů a při správě síťových účtů a sdílených zdrojů. Můžeme do ní zařadit následující prvky:

- **organizační jednotky** – jsou podskupinou domén, která často odráží funkční strukturu či strukturu organizace,
- **domény** – skupina počítačů, které se dělí o databázi adresářů,
- **doménový strom** – jedna či více domén, které sdílí spojitý jmenný prostor,
- **doménová struktura** – jedna či více domén, které mezi sebou sdílí informace o adresářích (Stanek, 2015).



Obrázek 2.3: Vícedoménová uspořádání. Zdroj: Horák 2011.

Organizační jednotky (OU) jsou podskupiny, které v doménách odráží funkční či obchodní strukturu. Mezi další důvody, proč organizační jednotky používat patří že:

- pomocí organizačních jednotek lze přiřadit zásady skupin malým skupinám zdrojů, aniž by bylo nutné aplikovat zásady na celou doménu,
- organizační jednotky vytváří menší, snáze spravovatelné pohledy na adresářové objekty v doméně,
- umožňují přenášet oprávnění a snadno řídit přístup správce ke zdrojům domény (Stanek, 2015).

- **Uživatelské účty**

Správa účtů je jedním z hlavních úkolů správce systému Microsoft Windows. Prostřednictvím uživatelských účtů lze jednotlivým uživatelům umožnit přihlašovat se k síti a přistupovat k síťovým zdrojům.

- **Skupiny uživatelů**

Stanek (2015, s. 345) uvádí, že „*skupiny udělují oprávnění podobným typům uživatelů a zjednodušují správu účtů. Pokud je uživatel členem skupiny, která má přístup k prostředkům, může k daným prostředkům přistupovat také. Uživateli je tak možné udělit potřebná oprávnění pouze jeho přiřazením do vhodné skupiny.*“

Skupiny Active Directory mohou mít různé rozsahy, které určují oblast, v níž skupina platná.

- **Místní doménové skupiny** – skupiny, kterým mohou být udělena oprávnění pouze v rámci jediné domény. Členové mohou být z libovolné domény dané struktury či z důvěryhodných domén jiných struktur.
- **Pevné místní skupiny** – jsou to skupiny, které nelze vytvářet ani odstraňovat. Lze je pouze upravit. Jsou to skupiny se speciálním rozsahem, které mohou mít oprávnění v místní doméně.
- **Globální skupiny** – skupiny sloužící k určení uživatelů a počítačů jedné domény a sdílející podobné role, funkce a úkoly. Mezi členy globální skupiny mohou patřit pouze účty a skupiny z domény, ve které je skupina vytvořena.
- **Univerzální skupiny** – tyto skupiny se používají pro označení uživatelů a počítačů v jedné doméně. Takto označení uživatelé a počítače by měli mít široké oprávnění v celé doménové struktuře. Členové těchto skupin mohou být účty, globální skupiny a další univerzální skupiny z jakékoli domény v doménové struktuře (Stanek, 2015).

- **Zásady skupiny**

Zásady si lze představit jako sadu pravidel, pomocí kterých je možné spravovat uživatele a počítače. Lze je používat pro několik domén nebo pro jednotlivé domény, pro dílčí skupiny v rámci domény nebo pro jednotlivé systémy. Zásady skupiny zjednodušují správu tím, že správcům umožňují centralizované řízení oprávnění a možností uživatelů i počítačů.

Stanek (2015, s. 160) uvádí, že „prostřednictvím zásad skupiny můžete provádět následující úlohy:

- *kontrolovat přístup k součástem systému Windows, systémovým prostředkům, síťovým prostředkům, nástrojům v Ovládacích panelech, ploše a obrazovce Start,*
- *vytvářet centrálně spravované adresáře pro zvláštní složky, například uživatelskou složku Dokumenty,*
- *definovat skripty uživatelů a počítačů, které se mají spouštět ve stanovených dobách,*
- *konfigurovat zásady pro uzamknutí účtů a hesel, auditování, přiřazení uživatelských práv a zabezpečení.“*

#### **b) DHCP Server**

Protokol DHCP (Dynamic Host Configuration Protocol) usnadňuje správu domény Active Directory. Pomocí protokolu DHCP se dynamicky přiřazuje síťovým klientům konfigurace protokolu TCP/IP. Zejména IP adresa, maska podsítě, výchozí brána a primární a sekundární DNS servery. Po instalaci je nutné nadefinovat obory, se kterými bude server pracovat a které bude zapůjčovat připojeným klientům (Stanek, 2015).

#### **c) DNS Server**

DNS je služba, převádějící názvy počítačů na IP adresy a rozřazující skupiny počítačů do domén. Hierarchie DNS domén je definována v celé síti Internetu. Jednotlivé úrovně hierarchie pak identifikují počítače, organizační domény a domény nejvyšší úrovně (Stanek 2015).

Dále Stanek (2015) uvádí, že systém DNS je interní součástí technologie Active Directory, a to do takové míry, že před instalací služby Active Directory je nejprve nutné nakonfigurovat službu DNS.

## 2.6. Virtual Private Network

Virtuální privátní sítě vytvářejí bezpečné linky z nezabezpečených spojení. Virtuální okruhy, které takto vzniknou, jsou privátní datovou sítí propojující uživatele nebo lokality prostřednictvím veřejné sítě s pomocí tunelovacích a šifrovacích protokolů (Sosinsky, 2010).

Z hlediska charakteru můžeme VPN rozdělit zhruba na následující čtyři typy:

- **interní linky v místní síti LAN** – jde o VPN spojení mezi dvěma počítači v jediné místní síti,
- **linky mezi místními sítěmi LAN** – VPN síť v tomto případě propojuje dvě různé místní sítě LAN,
- **externí linky prostřednictvím rozlehlé sítě WAN** – spojení mezi dvěma vzdálenými místními sítěmi LAN prostřednictvím rozlehlé linky WAN,
- **linka pro vzdálený přístup** – jedná se o přechodná spojení přes rozlehlou síť WAN, kterou se vzdálený klient připojuje k místnímu serveru nebo síti (Sosinsky, 2010).

Sosinsky (2010, s. 727) píše, že „*IPsec je sada protokolů, které mohou sloužit k zapouzdření komunikace protokolem IP do tunelů. Účelem je umožnit vzdálený přístup klientům nebo vzájemné propojení sítí. Přitom IPsec musí fungovat nejen na koncových bodech VPN linky, ale také na mezilehlých firewallech a všech dalších zařízeních na trase, která mají funkci směrovačů.*“

Mezi další protokoly používané k navázání vzdálené připojení patří také protokol PPTP. Jedná se o linkový protokol druhé vrstvy, s jehož pomocí lze vytvářet tunely pro vzdálený přístup a zasílání PPP dat mezi uživatelem a VPN bránou či koncentrátorem. PPTP tunel lze nastavit tak, že přístup je umožněn celému vzdálenému síťovému segmentu (Sosinsky, 2010).

## 2.7. Zabezpečení sítě

Každá síť je denně ohrožena stále propracovanějšími útoky a viry. Pro kvalitní síťové zabezpečení, je třeba zapojit několik technologií na různých vrstvách, které se částečně překrývají. Je potřeba zabezpečit místní síť od celosvětové sítě a také bezdrátové připojení k síti.

## a) Zabezpečení lokální sítě

Pro zabezpečení lokální sítě lze využít různých metod a způsobů. Mezi ty nejzákladnější patří využití Firewallu. Firewally vyhodnocují přes ně procházející síťový provoz a rozhodují se, kterou komunikaci předat dále a kterou zablokovat nebo vrátit zpět. Kritériem pro takové rozhodování je filtr. Zadání pro filtr může být založeno na informacích ze záhlaví paketu, zejména zdrojové a cílové adresy, protokolu a dalších faktorech (Sosinsky, 2010).

Thomas (2005, s. 140) uvádí, že mezi nejběžnější pravidla činností firewallů patří:

- **„Blokování příchozího síťového provozu podle jeho zdroje nebo cíle.** *Zablokování nežádoucího příchozího provozu je nejběžnější funkcí firewallu a je konec konců hlavním důvodem pro jeho instalaci – zabránit vstupu nežádoucího provozu do vnitřní sítě. Takovýto provoz obvykle pochází od útočníků, takže jej budeme chtít určitě rychle vykázat pryč.*
- **Blokování odchozího síťového provozu podle jeho zdroje nebo cíle.** *Řada firewallů dokáže sledovat také síťový provoz ve směru z vnitřní sítě do veřejného Internetu; takto můžeme například zaměstnancům vlastní firmy zabránit v přístupu k nevhodným webovým stránkám.*
- **Blokování síťového provozu podle obsahu.** *Vyspělejší firewally sledují v síťovém provozu také nepřipustný obsah. S firewallem může být například integrován antivirový program, který zabraňuje virům ve vstupu do vnitřní sítě.*
- **Zpřístupnění zdrojů vnitřní sítě.** *Primárním úkolem firewallu je sice zabránit v průchodu nežádoucího síťového provozu, u většiny z nich můžeme ale také nakonfigurovat selektivní povolení přístupu ke zdrojům (prostředkům) vnitřní sítě, jako je například veřejný webový server.*
- **Povolení některých spojení do vnitřní sítě.** *Zaměstnanci se do podnikové sítě běžně připojují také prostřednictvím virtuální privátní sítě. Tyto sítě umožňují bezpečné připojení z Internetu, například pro domácí pracovníky.*
- **Oznamování průběhu síťového provozu a činnosti firewallu.** *Při monitorování síťového provozu do a z Internetu je také důležité vědět, co všechno firewall dělá a kdo se pokouší „nabourat“ do vnitřní sítě a kdo se pokouší na Internetu přistupovat k nevhodnému materiálu.“*

## **b) Zabezpečení bezdrátové sítě**

První úroveň zabezpečení bezdrátové sítě je identifikátor SSID. Přístupový bod vysílá identifikátor SSID každých několik sekund v takzvaném majákovém rámci. Takto může oprávněný uživatel snadno najít správnou síť, ale zároveň se do ní dostane i neoprávněný útočník. Právě díky této funkci dokáže většina softwarových detekčních nástrojů najít bezdrátovou síť bez předchozí znalosti SSID. Je vhodné ihned po spuštění bezdrátové sítě změnit tovární hodnotu na jiný, hůře odhadnutelný text (Thomas, 2005).

Další možností, kterou lze využít pro zabezpečení bezdrátové sítě je využití protokolu WEP (Wired Equivalent Privacy), tedy soukromí ekvivalentní s kabelovým přenosem. Jedná se o minimální úroveň zabezpečení. Tento protokol zajišťuje šifrování dat v rámci 802.11 s pomocí symetrické šifry RC4. Pracuje se 40 bitovými nebo 104 bitovými klíči a jedná se o algoritmus proudového šifrování dat v bezdrátovém spojení (Sosinsky, 2010).

Velmi brzo po vydání protokolu WEP si uživatelé i výrobci začali uvědomovat jeho nedostatky. Pro získání nejvyšší bezpečnosti byla zavedena nová norma, jejímž základem byl protokol WPA (Wi-Fi Protected Access). Mezi jeho hlavní znaky patří: průběžná a automatická výměna dynamicky vytvářených klíčů pro šifrovací procedury (což vyřešilo zásadní slabinu technologie WEP). Druhým vylepšením je zvětšení délky klíče pro šifrování na hodnotu až 256 bitů. Posledním zdokonalením je MAC filter, který umožňuje povolit přístup do sítě pouze vybraným uživatelům na základě vypsání fyzické adresy jejich Wi-Fi zařízení (Horák, 2011).

### **3. Analýza současného stavu počítačové sítě**

Tato kapitola bude zaměřena na bližší představení Základní školy v Hrabyni a její charakteristiku. V následující části bakalářské práce bude také zachycen současný stav síťové architektury a jeho nedostatky a v neposlední řadě také požadavky školy.

#### **3.1. Informace o škole**

V devadesátých letech minulého století byla provedena rozsáhlá rekonstrukce školní budovy, která pochází z konce 19. století.

V roce 1996 byla zahájena výuka v nové přístavbě školy. Vznikla nová, moderní, prosvětlená budova, vybavena novým funkčním školním nábytkem a o rok později, v roce 1997, byly pořízeny první tři počítače. Zároveň byla opravena stará budova školy, do přízemí byly později přestěhovány kanceláře Obecního úřadu Hrabyně. Horní patro využívá základní škola.

V současné době školu navštěvuje 70 žáků a výuka probíhá v nové budově ve čtyřech třídách. V přízemí se nachází šatny, výdejna stravy, školní družina, sociální zařízení a počítačová učebna a v prvním jsou umístěny učebny, kabinet učitelů, sborovna, ředitelna, sociální zařízení a herna. Ve staré části budovy se nachází učebna 4. ročníku a herna tělesné výchovy.

Z projektů EU bylo za školou postaveno nové multifunkční hřiště a modernizováno vybavení školy, kdy byly do každé učebny pořízeny interaktivní tabule a do PC učebny další počítače. V současné době škola disponuje 25 počítačovými stanicemi, v PC učebně je umístěn počítač pro učitele a dalších 15 stanic pro žáky, dále jeden v každé ze čtyř tříd, tři v kabinetu učitelů, jeden v ředitelně a jeden ve školní družině.



### **3.2. Představa školy o zlepšení**

Hlavním důvodem investic do IT vybavení je veliké množství výukových programů, které žákům zpestřují studium a učitelům slouží jako nástroj pro obohacení výuky. Vzhledem k tomu, že počet různých výukových programů roste a škola pořizuje stále další, roste také náročnost na kapacitu a hardwarovou konfiguraci koncových stanic.

Vedení Základní školy v Hrabyni se rozhodlo pro pořízení a implementaci síťového operačního systému s dostatečnou konfigurací, aby byl vyřešen problém s častou modernizací koncových stanic. Výukové programy se nainstalují na server, a z koncových stanic se budou pouze spouštět. Nároky na jejich hardwarovou konfiguraci budou tedy zanedbatelné. S instalací programů pouze na server je také spojeno ušetření finančních nákladů na zakoupení licencí.

Dalším aspektem zlepšení, který implementace serveru přinese, je možnost propojení počítačů a vytvoření síťových účtů, kdy budou vytvořeny osobní účty pro každého učitele a každého žáka 4. a 5. ročníku. Vzhledem k tomu, že učitelé často vyučují každou hodinu v jiné třídě, jsou nuceni si po skončení každé hodiny vzít své materiály s sebou na přenosném paměťovém zařízení. Zavedení serveru do sítě tento problém eliminuje. Učitelé budou mít přístup ke svým materiálům z kteréhokoli počítače, k němuž se přihlásí pod svým síťovým účtem.

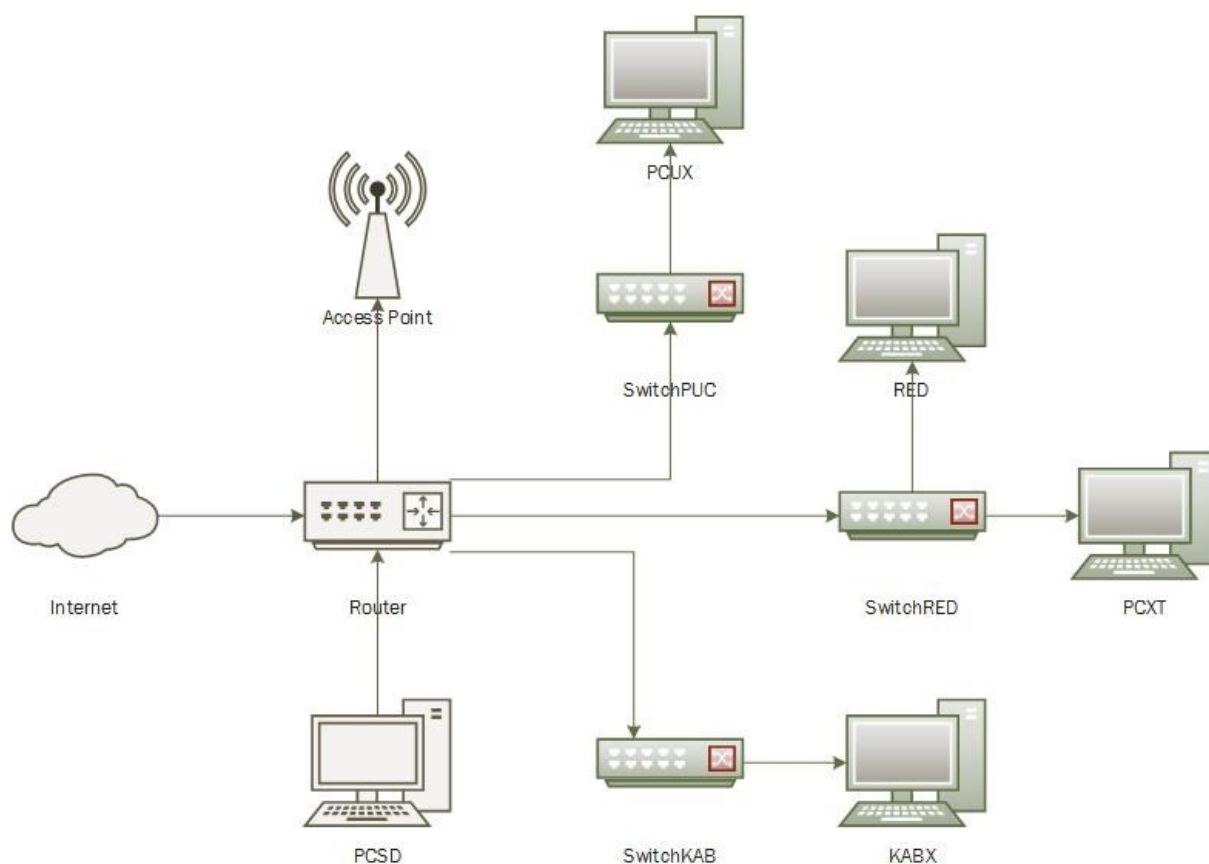
Vedení školy si přeje vytvořit osobní účty pouze pro žáky vyšších ročníků, jelikož v nižších ročnících by bylo využití účtu zanedbatelné. Pro žáky nižších ročníků bude na každé stanici v počítačové učebně vytvořen univerzální lokální studentský účet.

Učitelé budou mít také přístup ke svým materiálům a síťovým složkám z domova díky zřízenému vzdálenému přístupu pomocí VPN. Nebudou již muset nosit USB flash disky či jiná paměťová zařízení. Přípravu na výuku budou moci tvořit doma na svých osobních počítačích a poté se pomocí virtuální privátní sítě připojí ke školnímu serveru a uloží si připravené materiály do své síťové složky. Ve škole se potom jednoduše na kterémkoli počítači přihlásí pod svým doménovým účtem a své materiály si budou moci otevřít či stáhnout do počítače, u kterého právě pracují.

### **3.3. Popis současného stavu**

Jak bylo zmíněno v textu výše, modernizace počítačů probíhala kontinuálně v závislosti na množství a náročnosti nakupovaných výukových programů a příležitostně se z rozpočtu obce a dotací rozšiřoval jejich počet.

Ve škole se v přízemí nacházejí šatny, sociální zařízení, výdejna stravy, školní družina s jedním počítačem a počítačová učebna s šestnácti počítači, kde probíhá výuka v rámci hodin informatiky. V prvním patře, ve staré části budovy se nachází herna tělesné výchovy a učebna 4. ročníku a v nové tři třídy pro klasickou výuku. V každé třídě jsou instalovány interaktivní tabule a PC pro její ovládání. Naproti tříd najdeme hernu, sborovnu, kabinet učitelů, ředitelnu a sociální zařízení.



Obrázek 3.1: Schéma stávající školní sítě. Zdroj MS Visio, vlastní zpracování.

Současné schéma sítě zachycuje obrázek 3.1. Internetové připojení je v počítačové učebně svedeno do routeru, na který jsou potom dále připojeny další aktivní prvky – switche a počítač ve školní družině. První switch se nachází přímo v počítačové učebně a na něj je připojeno 15 žákovských stanic a učitelský PC, další se nachází v kabinetu ředitele a do něj jsou zapojeny počítače ze všech tříd. Poslední switch je umístěn v kabinetu učitelů.

Vzhledem k tomu, že počítač v učebně 4. ročníku se nachází ve staré části budovy, je do sítě připojen pomocí bezdrátového Access Pointu, který zároveň poskytuje bezdrátové připojení po celé budově. Tohoto bezdrátového Wi-Fi připojení, je využíváno zejména při práci s tablety a interaktivními tabulemi. Toto řešení bude zachováno i po modernizaci, jelikož

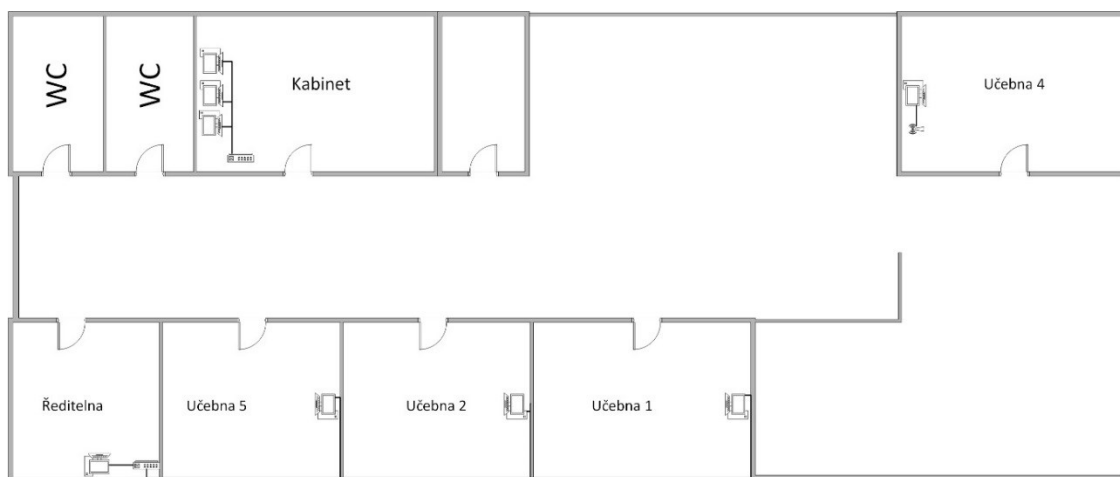
kabelové připojení tohoto počítače do sítě by znamenalo značné komplikace a náročnější stavební úpravy, kterým by se chtělo vedení školy vyhnout.

Veškerá kabeláž potřebná pro propojení aktivních prvků se stanicemi je vedena ve stropních a nástěnných lištách.

Schéma rozmístění počítačů, aktivních prvků a vedení kabeláže v obou patrech školy je zobrazeno na obrázcích 3.2 a 3.3.



Obrázek 3.2: Schéma přízemí školní budovy. Zdroj MS Visio, vlastní zpracování.



Obrázek 3.3: Schéma prvního podlaží školní budovy. Zdroj MS Visio, vlastní zpracování.

### **3.4. Specifikace požadavků**

Po vzájemné komunikaci s vedením základní školy, byly vymezeny hlavní požadavky. Vedení požaduje modernizaci stávající sítě bez větších stavebních úprav, pokud možno tak s využitím stávajících prvků.

Jelikož jedním z cílů inovace sítě je omezit neustálou modernizaci koncových stanic, z důvodu narůstajících požadavků na výpočetní výkon ze strany výukových programů, požaduje škola nainstalovat tyto programy na jednu dostatečně výkonnou serverovou stanici, odkud se budou tyto programy pouze spouštět.

Dále vedení školy požaduje vytvořit vlastní síťové účty pro zaměstnance a žáky vyšších ročníků, zejména proto, aby učitelé měli přístup ke svým materiálům ze všech počítačů ve škole a nemuseli již u sebe nosit přenosná paměťová zařízení a pro žáky mimo jiné pro to, aby se naučili používat své vlastní účty a viděli, jak funguje práce s počítačem v doméně a jaké to s sebou nese výhody a nevýhody.

S tímto je spojeno také omezení žákovských účtů tím způsobem, aby žáci nemohli neopatrnou manipulací či nešťastnou náhodou poškodit konfiguraci počítačové stanice či celé sítě. Je požadováno, aby data, která budou ukládána učiteli a žáky na server, byla v určitém intervalu automaticky zálohována.

Mezi další požadavky patří zajištění síťové tiskárny, na které by mohli žáci v počítačové tisknout své dokumenty, její zapojení a nastavení a v neposlední řadě také umožnění pedagogům přistupovat z domova ke svým materiálům uloženým na serverové stanici.

## **4. Návrh lokální počítačové sítě**

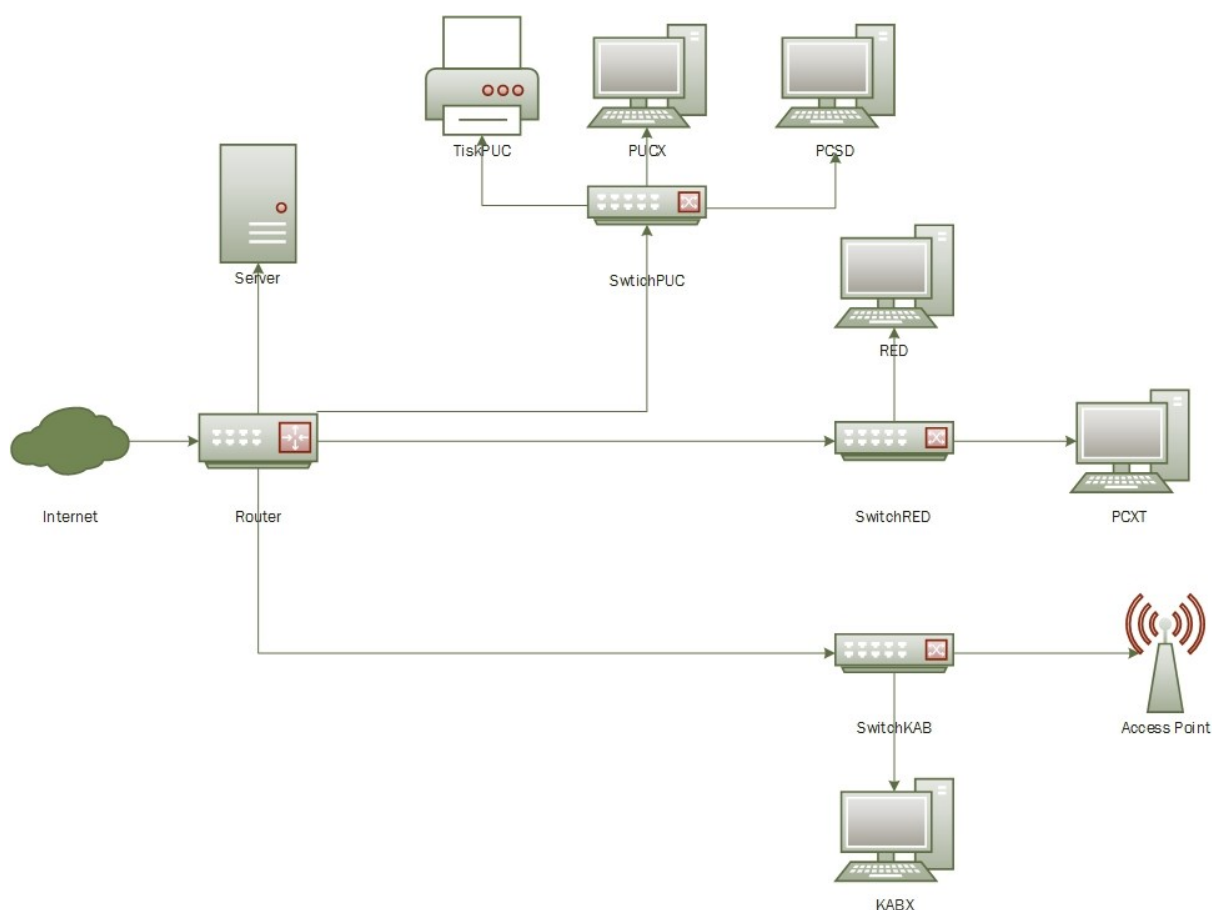
V této kapitole bude vytvořen návrh na rozšíření a modernizaci stávající lokální počítačové sítě tak, aby uspokojil všechny požadavky vedení Základní školy Hrabyně.

### **4.1. Návrh sítě**

Pro splnění všech požadavků, jež jsou na síť kladeny, bude ji nutné postavit na architektuře klient-server. Do stávajícího řešení bude připojena serverová stanice se síťovým operačním systémem, která bude umístěna v počítačové učebně. Všechny počítače ve všech učebnách a kabinetech budou se serverem komunikovat.

Vzhledem ke zvolené architektuře, bude mít fyzická topologie sítě podobu hvězdy. Přesněji bude použita Rozšířená hvězdicová topologie, jelikož každý uzel, do kterého povede kabel od centrálního uzlu, bude středem další hvězdy. Páteční spoje budou posíleny a síť bude odpovídat standartu 1000Base-T, tedy Gigabitový Ethernet. Centrálním prvkem sítě bude router, umístěný v počítačové učebně. Do něj pak bude připojena serverová stanice a tři další aktivní prvky – switche. Přepínače zabezpečí, aby pakety nebyly vysílány na všechny připojené stanice, ale podle MAC adresy bude přesně určena stanice, které pakety náleží.

První switch zabezpečí síťovou komunikaci s počítači v počítačové učebně a školní družině, další switch s počítači v učebnách a ředitelně a poslední přepínač zabezpečí komunikaci s počítači v kabinetu učitelů. Použití této topologie má několik výhod. Mezi hlavní výhody patří jednoduchost případného rozšíření a také nastavení celé sítě, dále se v této topologii snadno hledají závady a v neposlední řadě rovněž platí, že pokud selže jedna stanice nebo kabel, nebude fungovat spojení pouze pro jednu stanici. Ostatní stanice mohou nadále komunikovat. Toto řešení má ovšem také nevýhody. Hlavní nevýhodou použití této topologie je obrovská závislost na centrálním uzlu. V případě selhání centrálního síťového prvku, v našem případě se jedná o router, do kterého jsou všechny ostatní prvky připojeny, přestane fungovat celá síť.



Obrázek 4.1: Schéma fyzické topologie navrhované sítě. Zdroj: MS Visio, vlastní zpracování.

Vysvětlivky označení prvků sítě:

- SwitchPUC – switch v počítačové učebně,
- PCSD – počítač ve školní družině,
- PUCX – počítače v počítačové učebně,
- TiskPUC – tiskárna v počítačové učebně,
- SwitchRED – switch v ředitelně,
- SwitchKAB – switch v kabinetu,
- RED – počítač v ředitelně,
- KABX – počítače v kabinetu,
- PCXT – počítač ve třídě.

## 4.2. Volba nových prvků sítě

Jak již bylo zmíněno v předchozí kapitole, vedení školy si přeje implementovat serverové řešení do své sítě také z důvodu časté modernizace koncových stanic. Po zapojení serveru se tedy nepředpokládá další modernizace stávajících klientských počítačů.

Je nutné zakoupit nové aktivní prvky, zejména nový router, který dokáže zajistit vzdálené připojení přes virtuální privátní síť a také switch do počítačové učebny s dostatečným počtem portů, aby byla škola připravena na případné rozšíření stávajícího počtu klientských počítačů.

Klíčový bude také výběr vhodné, výkonné stanice, na které bude nainstalován síťový operační systém.

Škola je ze zákona povinna na nákup těchto komponent vypsát výběrové řízení, proto následující položky jsou pouze doporučené a mohou být změněny.

### 4.2.1. Aktivní prvky sítě

Po analýze trhu a současné nabídky bylo škole navrženo zakoupit tyto aktivní prvky:

- Router – TP-LINK TL-R600VPN: Toto zařízení je opatřeno celkem 5 gigabitovými porty, ze kterých je 1 WAN port a 4 LAN porty, čímž uspokojí potřeby k přístupu na internet z více zdrojů. Router podporuje funkci VPN a nabízí jako ochranu proti externím hrozbám funkci Firewall SPI. Kromě toho může automaticky rozpoznat a zablokovat útoky DoS, jako jsou například Ping of Death a jiné podobné hrozby. Tento router také poskytuje funkce filtrování IP/MAC adres a názvů domén, které důrazně brání útokům narušitelů a virů.
- Switch – TP-Link TL-SG1024: Tento switch disponuje 24 porty s rychlostí až 1000 Mbps. Je určen do menších a středně velkých sítí. Zařízení podporuje nejrozumnější síťové protokoly a samozřejmě také detekce kabelů, či informační LED dioda pro jednotlivé porty.

Bude zakoupena cenově dostupná černobílá laserová tiskárna, která bude rovněž zapojena do sítě v počítačové učebně a bude sloužit žákům ke studijním účelům. Tisk z učitelských stanic v současné době zajišťují čtyři malé tiskárny, přímo připojené ke stanicím. Toto bude zachováno, ale do budoucna je navrženo pořízení a zapojení druhé síťové tiskárny, jež tyto malé tiskárny nahradí.

Pro distribuci Wi-Fi připojení bude využito stávajících prvků, které jsou již do sítě zapojeny.

#### **4.2.2. Serverová stanice**

Nejdůležitějším prvkem celé sítě bude stanice, na které bude nainstalován síťový operační systém. Je nutno zvolit variantu splňující veškeré požadavky vedení školy, zejména dostatečnou konfiguraci a kapacitu pro mnohé výukové programy.

Po zvážení různých možností vedení školy doporučuji server od firmy Hewlett-Packard, HP ProLiant ML30 Gen9. Tento jednoprocessorový server je vhodný zejména pro menší, rozvíjející se podniky, ke kterým lze základní školu přirovnat. Dokáže bezproblémově zpracovat veškeré serverové úlohy, jako je běh kancelářských, výukových či jiných aplikací. Zpracování komponent by mělo uspokojit nároky na spolehlivost, vzhledem k téměř nepřetržitému běhu systému. Technické parametry tohoto modelu jsou následující:

- čtyřjádrový procesor Intel Xeon E3-1220 v5 pokročilé architektury Skylake. Procesor funguje na frekvenci 3,0 GHz a v případě zátěže až na 3,5 GHz,
- 8 GB operační paměti typu DDR4 o frekvenci 2133 MHz, přičemž celkem jsou k dispozici celkem 4 paměťové sloty (až 64 GB),
- dvojice 1 TB pevných disků SATA non-hot-plug o rychlosti 7200 otáček, které se dají rozšířit do pole RAID 0/1/5/10,
- 2x USB 2.0, 6x USB 3.0 a VGA D-SUB výstupy,
- pro připojení k síti je dostupná duální síťová karta s rychlostí až 1 Gbps. Vzdálenou správu lze efektivně provádět přes moderní komunikační standard iLo.

HP Integrated Lights-Out je nástroj pro vzdálenou správu přes webové rozhraní. Síťová karta iLO má vlastní napájení a oddělené síťové připojení (vlastní IP adresu). Je proto možné například server zapnout na dálku, i když zrovna neběží. Dále je také možné server restartovat nebo spustit vzdálenou plochu či příkazový řádek.

Server disponuje již v základu dvojicí disků o celkové velikosti 2 TB, ale doporučuji dokoupit disk další, pro oddělení kompletního nastavení serveru a Active Directory, samotné instalace a uživatelských dat a zálohy.



### 4.2.3. Software

Při volbě síťového operačního systému připadají v úvahu dvě varianty (Novel NetWare nemá pro takto malou síť příliš smysl a jeho administrace je zbytečně náročná.) A to Windows Server a Linux. Po zvážení všech kladů a záporů a po konzultaci s budoucím správcem, se škola rozhodla zakoupit licenci Windows Server od společnosti Microsoft, která je sice dražší možností v porovnání s open-sourcovým systémem Linux, ale nabízí přívětivé uživatelské rozhraní a jednoduchou správu funkcí serveru. Dalším důvodem pro toto rozhodnutí jsou také výrazné slevy na zakoupení licencí produktů Microsoft pro školská zařízení.

### 4.3. Nastavení aktivních prvků

V této kapitole bude popsáno nastavení jednotlivých aktivních prvků v síti.

- **Router TP-LINK TL-R600VPN**

Router je bránou do internetu a klíčovým prvkem celé školní sítě. Je do něj připojena serverová stanice, přístupový bod, který rozvádí Wi-Fi připojení po škole a dva přepínače. Pokud by došlo k poruše na tomto zařízení, veškerá komunikace mezi stanicemi ve školní síti by přestala fungovat.

Funkce dynamického přidělování IP adres nebude na tomto zařízení využívána, jelikož tuto bude zastávat server, kde bude role DHCP nainstalována.

Položka	Hodnota
IP Adresa	192.168.1.2
Maska	255.255.255.0
Výchozí brána	192.168.1.1
Primární DNS	192.168.1.3

*Tabulka 4.1: Parametry nastavení routeru, pro připojení k internetu.*

- **Bezdrátový AP**

Tento bezdrátový Access Point se stará o distribuci Wi-Fi připojení po celé škole. Zařízení je poměrně nové a funkci plní obstojně, není tedy důvod jej měnit. Tento přístupový bod bude připojen k routeru a budou mu staticky přiděleny všechny údaje tak, aby mohl nadále distribuovat bezdrátové připojení.

<b>Položka</b>	<b>Hodnota</b>
IP Adresa	192.168.1.4
Maska	255.255.255.0
Výchozí brána	192.168.1.2
Primární DNS	192.168.1.3

*Tabulka 4.2: Parametry Wi-Fi připojení.*

Po připojení zařízení k síti Wi-Fi mu bude automaticky, jako všem ostatním zařízením v síti, přidělena IP adresa a další parametry připojení pomocí funkce DHCP, která bude nainstalována na serveru. Připojení bezdrátovým způsobem bude šifrováno heslem a protokolem WPA2-PSK.

#### **4.4. Připojení serveru**

Serverová stanice, podobně jako aktivní prvky bude do sítě připojena kabelem, a to do doporučeného routeru. IP adresa a další parametry připojení mu budou přiděleny staticky.

<b>Položka</b>	<b>Hodnota</b>
IP Adresa	192.168.1.3
Maska	255.255.255.0
Výchozí brána	192.168.1.2
Primární DNS	192.168.1.3

*Tabulka 4.3: Parametry připojení serverové stanice k síti.*

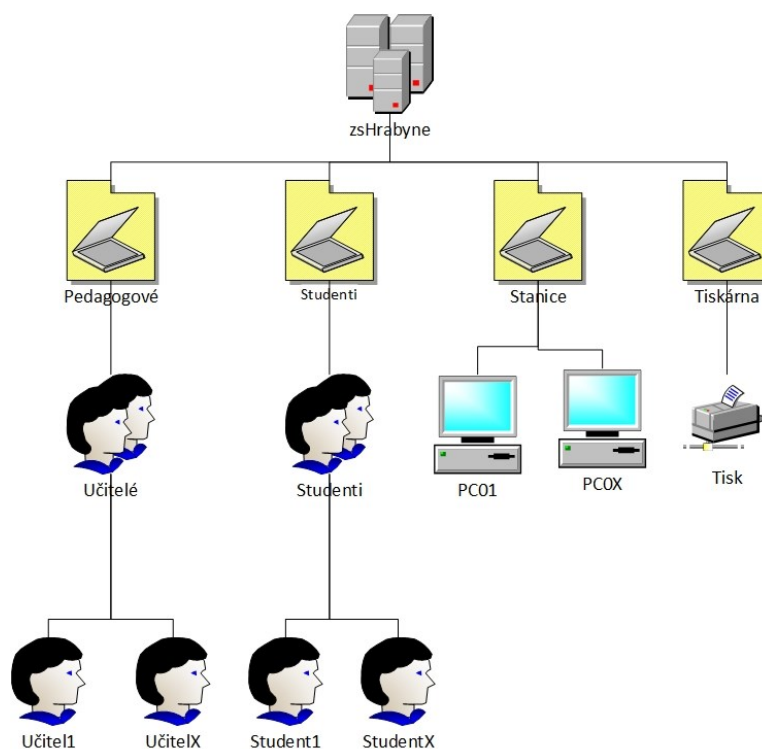
#### **4.5. Instalace a konfigurace rolí serveru**

Následující část je zaměřena na instalaci a konfiguraci rolí síťového operačního systému. Zejména na adresářovou službu Active Directory, funkci DHCP a DNS a nastavení tiskových služeb. Jeden z pevných disků bude sloužit pro ukládání dat učitelů a žáků do jejich síťových složek, a to z kterékoliv pracovní stanice ve škole, proto je nutné nastavit síťový přístup k těmto složkám a celkové zálohování dat.

### 4.5.1. Active Directory Domain Services

V rámci adresářové služby Active Directory bude vytvořena doména s názvem zsHrabyne. Jelikož je navrhovaná síť poměrně malá a půjde o prostředí s jednou doménou, bude se skládat z jednoho lesa o jednom stromu. Ve školní doméně budou vytvořeny čtyři organizační jednotky.

První OU Pedagogové bude obsahovat skupinu uživatelských účtů učitelů, druhá OU Studenti bude obsahovat skupinu uživatelských účtů žáků, třetí OU Stanice bude obsahovat veškeré koncové stanice připojené do domény a čtvrtá OU Tiskárna bude obsahovat síťovou tiskárnu. Žáci a učitelé budou mít vytvořenou svou vlastní organizační jednotku, jelikož práva skupin uživatelských účtů Učitelé a Žáci se budou lišit.



Obrázek 4.2: Schéma adresářové služby ADDS. Zdroj: MS Visio, vlastní zpracování.

S adresářovou službou Active Directory je úzce spjata funkce DNS, bez které doménový systém nemůže správně fungovat. Funkce bude nainstalována na serverové stanici a všechny ostatní připojené stanice do sítě, budou této funkci využívat. Konfigurace DNS proběhne automaticky v rámci instalace Active Directory.

- **Postup Instalace Active Directory:**

Na začátku je nutné změnit jméno serveru a nastavit mu pevnou IP adresu. Jelikož pevnou IP adresu již má, zbývá pouze změnit jméno.

Ve Správci serveru v levé části zvolíme položku Místní server a vybereme Název počítače. Pomocí tlačítka Změnit změním název serveru z výchozího názvu, který byl přidělen při instalaci na ZSHRABYNE. Po změně názvu serveru je potřeba provést restart.

Po restartu máme potřebnou konfiguraci hotovou a můžeme začít instalaci Active Directory. Přejdeme opět do Správce serveru a zvolíme položku Správa a v ní zvolíme Přidat funkce a role. Tlačítkem Další se dostaneme na další obrazovku, kde vybereme typ instalace, zvolíme Instalace na základě rolí nebo na základě funkcí a pak opět klikneme na Další.

Na další stránce klikneme na Vyberte server z fondu serverů, klikneme na název serveru, na který chceme nainstalovat službu AD DS, a pak na Další. Na stránce Vybrat role serveru zvolíme službu Active Directory Domain Services a DNS server, následně se objeví informace, že budou doinstalovány závislosti. Další okna instalace poskytují pouze informace a proklikáme se až k poslednímu oknu, kde spustíme instalaci.

Po pár minutách se instalace dokončí a na stránce Výsledky ověříme, že se instalace uskutečnila. Průvodce konfigurací služby Active Directory Domain Services spustíme tak, že klikneme na Povýšit tento server na řadič domény. V horní části Server Manageru uvidíme žlutý vykřičník a zvolíme volbu Přidat nový les.

Do kolonky Název kořenové domény napíšeme jméno nové domény, v našem případě bude jméno domény zsHrabyne.cz. Poté bude nutné zadat heslo pro mód obnovy, které si pečlivě uchováme. V dalším okně jsou implicitně nastaveny cesty k logovacím souborům, databázi a sysvol na disku C:\. Jelikož chceme mít celou Active Directory na zvláštním disku, změním cestu na disk D:\. Po instalaci řadiče domény se server do domény automaticky zaregistruje.

Instalace bude prováděna ve spolupráci s firmou 24IT s.r.o., která budou mít následnou správu na starost. Veškeré kritické informace a údaje při instalaci budou zdokumentovány a předány vedení školy a také budoucímu správci.

- **Organizační jednotky**

Jakmile bude Active Directory nainstalována, budeme moci vytvořit Organizační jednotky. Budou vytvořeny celkem čtyři. V první OU bude skupina uživatelských účtů učitelů, ve druhé OU bude skupina účtů žáků, ve třetí budou pracovní stanice a ve čtvrté bude síťová tiskárna.

Organizační jednotky obsahující skupiny uživatelských účtů budou mít přiřazeny zásady skupiny, které lze aplikovat na všechny skupiny účtů v dané Organizační jednotce.

Vytvoření nové Organizační jednotky provedeme v modulu Uživatelé a počítače služby Active Directory. Pravým tlačítkem klikneme na doménu, ve které chceme novou Organizační jednotku vytvořit, klikneme na položku Nová a vybereme možnost Organizační jednotka. Následně už jen zadáme název Organizační jednotky.

- **Zásady skupiny**

Pomocí Zásad skupiny můžeme hromadně spravovat oprávnění a nastavení, které může být aplikované jak na počítač, tak na uživatele.

V panelu Nástroje vybereme možnost Správa zásad skupiny. V nově otevřeném okně můžeme vidět strom domén, obsahující námi vytvořenou doménu. Po rozkliknutí naší domény vidíme již vytvořené Organizační jednotky, které propojíme s Objektem zásad skupiny. Pravým tlačítkem klepneme na první OU Učitelé a vybereme první možnost, a to Vytvořit objekt zásad skupiny v této doméně a propojit jej sem. Tento objekt pojmenujeme PedagogoveGPO. Obdobně vytvoříme objekt pro OU Studenti, který ponese název StudentiGPO.

Jakmile máme objekt zásad skupiny vytvořen, klepneme na něj pravým tlačítkem myši a vybereme Upravit. V následujícím okně máme možnost upravit nastavení jak pro počítače, tak pro uživatele. Pokud se zaměříme na uživatele, vidíme, že lze nastavit nejružnější omezení týkající se nastavení systému Windows, softwaru, předvoleb a tak dále. Objekt zásad skupiny PedagogoveGPO bude mít pro začátek nastaveno omezení instalace softwaru a dále také znemožněn přístup do správce úloh a také panelu nástrojů. Objekt zásad skupiny studentů bude mít omezení obdobná.

Při realizaci budou ve spolupráci s ředitelkou školy tato omezení rozšířena a zdokumentována, tak aby přesně odpovídala představě o tom, k jakým zdrojům může konkrétní skupina uživatelů přistupovat.

- **Uživatelské skupiny**

Uživatelské účty v naší doméně budou rozděleny do dvou Globálních skupin. První skupina bude v Organizační jednotce Pedagogové a bude obsahovat všechny uživatelské účty učitelů. Druhá skupina bude v Organizační jednotce Studenti a bude obsahovat veškeré uživatelské účty žáků.

Skupina Učitelé bude mít omezená práva, zejména právo na instalaci a odinstalaci programů. Skupině bude zachováno právo číst, zapisovat a spouštět. Rovněž bude mít tato skupina právo na tisk.

Skupina Studenti bude mít také omezená práva, ale ve větším měřítku. Opět bude mít odebrána práva na instalaci a odinstalaci programů, právo na čtení a zápis bude mít tato skupina pouze k síťové složce, která bude spojena s daným účtem, právo spouštět bude pouze pro vybrané aplikace. Tisk zakázán nebude.

Skupinu vytvoříme v Centru správy služby Active Directory. Pravým tlačítkem klikneme na příslušnou organizační jednotku a vybereme možnost Nový a poté Skupina. Dále zadáme název skupiny, rozsah skupiny zvolíme Globální a typ skupiny se zabezpečením.

- **Uživatelské účty**

Uživatelský účet umožňuje uživateli přihlásit se k počítačům a doménám s identitou, kterou je možné v doméně ověřit. Každý učitel nebo žák bude mít vytvořen svůj vlastní účet v dané skupině uživatelů, ten se bude skládat z prvních pěti písmen příjmení a prvních tří písmen křestního jména. V případě, že by došlo ke shodě s jiným účtem, poslední písmeno příjmení bude inkrementálně zvětšeno.

Při prvním přihlášení bude každý uživatel vyzván ke změně výchozího hesla, které bude nastaveno v podobě příjmení uživatele velkými písmeny a číslo 2017. Při tvorbě nového hesla budou muset být splněny dvě podmínky. A to že heslo musí obsahovat alespoň jednu číslici a alespoň jedno velké písmeno.

Výchozí účet Administrátor bude nahrazen novým doménovým účtem zadmin, který bude mít stejná administrátorská práva jako výchozí účet. K tomuto účtu bude mít přístup správce sítě a ředitelka školy.

Dále bude na každé stanici vytvořen lokální účet Student, který určený pro žáky nižších ročníků, kteří nebudou mít svůj vlastní síťový účet a také pro nouzové případy, kdy by nebylo možno se z nějakého důvodu pod doménovým účtem přihlásit.

- **Vytváření účtů**

Spustíme modul Centrum správy služby Active Directory. Následně klepneme pravým tlačítkem na Organizační jednotku, ve které budeme chtít nový účet vytvořit, najedeme na Nový a vybereme možnost Uživatel.

V okně Vytvořit účet v části účet následně provedeme tyto činnosti:

- do pole Jméno zadáme jméno nového uživatele,
- do pole příjmení zadáme příjmení uživatele,
- v poli Přihlašovací jméno bude zadáno přihlašovací jméno uživatele složené z pěti písmen příjemní a třech písmen jména
- a v poli Heslo a Potvrdit heslo bude nastaveno výchozí heslo, které si bude muset po prvním přihlášení každý uživatel změnit.

Pro vytvoření nových uživatelských účtů, bude nutno celý proces zopakovat, nebo zvolit možnost kopírování. Pokud klikneme pravým tlačítkem na již vytvořeného uživatele, můžeme vybrat možnost Kopírovat objekt – uživatel. Dále je třeba vyplnit jen jeho údaje, všechno ostatní je zkopírováno.

Uživatelské účty žáků budou mít omezeny počítačové stanice, ke kterým se budou moci svým účtem připojit. Abychom nemuseli nastavovat omezení u každého účtu zvlášť, využijeme možnosti hromadného nastavení. Až budeme mít vytvořeny všechny účty, otevřeme modul Uživatelé a počítače služby Active Directory, následně označíme všechny požadované účty, klikneme pravým tlačítkem a zvolíme Vlastnosti. Zde na kartě Účet zaškrtneme políčko Omezení počítače. Následně se proklikáme přes Připojit k až K následujícím stanicím, kde vyplníme názvy stanic, k nimž se bude možno těmito doménovými účty připojit.

V případě žákovských účtů to budou pouze stanice v počítačové učebně. V případě učitelských účtů takové omezení nebude, místo K následujícím stanicím zaškrtneme pole Ke všem pracovním stanicím.

- **Sdílené úložiště**

Každý účet vytvořený v rámci naší domény, bude mít přiřazenu svou osobní složku, označenou N:\, k této složce bude mít uživatel přístup ze kteréhokoliv počítače ve škole, ke kterému se přihlásí svým síťovým účtem. Velikost těchto složek bude omezena na 1,5 GB, jelikož se předpokládá ukládání vesměs textových souborů nepřesahujících několik megabytů.

Každý uživatel bude mít ke své složce neomezená práva, bude tedy moci zapisovat, číst i měnit uložené soubory.

Mimo osobní složku každého uživatele, budou vytvořeny ještě dvě další složky, které budou sloužit pro společné účely. Složka, která bude určena pro sdílení souborů mezi pedagogy, ponese označení P:\ a její velikost bude omezena na 50 GB. Učitelé budou mít v této složce možnost čtení a zápisu. Žáci do této složky nebudou mít vůbec přístup. Složka určená pro sdílení souborů mezi učiteli a žáky bude označena písmenem O:\. Její velikost bude omezena na 100 GB. Učitelé budou mít v této složce práva na čtení a zápis, žáci budou moci v této složce pouze číst.

Disk s uloženými daty uživatelů, bude rozdělen na tři oddíly. První oddíl bude vymezen pro složky uživatelů a další dva pro společná úložiště. Všechny tyto oddíly budou nasdíleny do sítě. Toto sdílení se nastaví na kartě Sdílení ve vlastnostech každého oddílu, kde bude nutné zadat síťovou cestu k disku. Pro oddíl s uživatelskými složkami (N:) to bude \\ZSHRABYNE\SlozkyUzivatelu, pro společný disk učitelů to bude \\ZSHRABYNE\DiskUcitele a pro společné úložiště pro žáky a učitele to bude \\ZSHRABYNE\DiskSpol.

Pro automatickou správu přiděleného místa uživatelským složkám bude vytvořena kvóta, která při vytvoření každé nové uživatelské složky zajistí, aby ji byla přiřazena požadovaná velikost. Pro nastavení kvót slouží funkce File Server Resource Manager, tuto bude nutno nainstalovat přes správu funkcí a rolí serveru. Poté ve Správci prostředků souborového systému bude vytvořena šablona s velikostí 1,5 GB, která bude přiřazena oddílu s uživatelskými složkami.

Nově vytvořená složka se poté sváže s uživatelským účtem v modulu Uživatelé a počítače služby Active Directory. Na kartě Profil ve vlastnostech uživatele zvolíme písmeno N:\ a zadáme cestu \\ZSHRABYNE\SlozkyUzivatelu\%USERNAME%. Na základě těchto údajů operační systém automaticky vytvoří složku pro daného uživatele.



### 4.5.2. Dynamic Host Configuration Protocol

DHCP protokol, který bude na serveru nainstalován spolu se službou Active Directory a DNS bude sloužit pro přidělování údajů nezbytných pro připojení stanic zapojených v síti.

Služba DHCP bude přidělovat IP adresy ve dvou rozsazích. První rozsah bude určen pro zařízení, která budou připojena k síti pevně, pomocí kabelu a druhý rozsah bude sloužit pro zařízení připojená pomocí bezdrátového Wi-Fi připojení.

Konfigurace těchto rozsahů je uvedena v tabulkách níže.

Položka	Hodnota
Počáteční IP adresa rozsahu	192.168.1.10
Koncová IP adresa rozsahu	192.168.1.60
Typ	Pevná síť

*Tabulka 4.4: Rozsah IP adres pro kabelově připojená zařízení.*

Položka	Hodnota
Počáteční IP adresa rozsahu	192.168.100
Koncová IP adresa rozsahu	192.168.1.199
Typ	Wi-Fi

*Tabulka 4.5: Rozsah IP adres pro bezdrátově připojená zařízení.*

Aktivní prvky v síti spolu s tiskárnou budou mít IP adresu přidělenou staticky pomocí rezervací v nastavení protokolu DHCP. Statická IP adresa u tiskárny je nutná z důvodu správného nastavení tiskového serveru.

- **Postup instalace a nastavení služby DHCP**

Přejdeme do Správce serveru a v nabídce Správa zvolíme Přidat role a funkce. Z nabídky vybereme možnost DHCP server a přejdeme k instalaci. Po úspěšné instalaci se v horní části Správce serveru objeví žlutý trojúhelník s informací o právě nainstalované službě DHCP. Provedeme restart serveru, po kterém znovu přejdeme do Správce serveru.

V záložce Nástroje najdeme a zvolíme možnost DHCP. V nově otevřeném okně klikneme pravým tlačítkem myši na možnost IPv4 a vybereme Nový obor. V průvodci konfigurací zvolíme název nového oboru, v našem případě Kabel či Wi-Fi, a v dalším okně

rozsah IP adres. V dalších oknech průvodce poté ještě postupně zvolíme IP adresu výchozí brány, kterou je námi použitý router a adresu DNS serveru, kterou představuje IP adresa serverové stanice. Na závěr aktivujeme námi vytvořený obor.

### **4.5.3. Tiskový server**

Síťová tiskárna bude umístěna v počítačové učebně a bude připojena ke switchi a její IP adresa bude nastavena staticky na hodnotu 192.168.1.6. Nastavení IP adresy na statickou hodnotu je nezbytné pro správné fungování tiskového serveru. Ten zabezpečí tisk na této tiskárně ze všech stanic připojených do domény. Bude možné tisknout ze všech uživatelských účtů včetně těch žákovských, jelikož žáci budou mít přístup do učebny pouze v přítomnosti vyučujícího, ten bude mít dohled nad tím, co žáci tisknou. Tiskárny v ředitelně a sborovně zůstanou nadále k dispozici učitelům. Jejich výměna za jednu síťovou tiskárnu je uvažována do budoucna.

### **4.5.4. Sdílení výukových programů**

Z důvodu, aby se výukové programy nemusely vždy instalovat na všechny klientské stanice a aby nebylo nutné je pro jejich výkon často modernizovat, rozhodlo se vedení školy, že se výukové programy nainstalují na dostatečně výkonnou serverovou stanici, odkud se budou pouze spouštět.

Sdílení bude zabezpečeno pomocí služby Vzdálená plocha a následného publikování vybraných programů. Toto řešení není vzhledem k bezpečnostním rizikům doporučováno a před několika lety ani nebylo možné. Vhodnějším řešením by byla instalace dvou serverů, jednoho jako řadiče domény a druhého jako zprostředkovatele vzdálené plochy. V případě tak malé organizace jako je základní škola, je bohužel toto řešení z finančního hlediska nemyslitelné, a proto je tedy volena tato možnost.

Nejprve je třeba nainstalovat Zprostředkovatele k vzdálené ploše. V modulu Správce serveru vybereme možnost Přidat role. Následně v části Vzdálená plocha a pokračujeme až k výběru služeb role. Zde zaškrtneme pouze možnost Zprostředkovatel připojení k vzdálené ploše. Po instalaci této služby znovu spustíme instalaci Vzdálené plochy a na místě Zprostředkovatele připojení k VP již vidíme náš server. Následně pokračujeme v instalaci a tentokrát vybereme i další služby, a to Hostitel relací VP a Webový přístup k VP.

Nyní je už možné publikovat vybrané programy pomocí aplikace RemoteApp. V Nástrojích pro správu vybereme možnost Vzdálená plocha a dále položku Správce aplikací

RemoteApp. V podokně Akce zvolíme možnost Přidat aplikace RemoteApp a dále už jen vybereme programy, které chceme sdílet.

#### **4.5.5. Zálohování**

Zálohování bude prováděno každý den. Jelikož se v rámci sítě nebude pracovat s důležitými daty, zálohování vícekrát denně nebude potřeba. Zálohování bude spouštěno ve večerních hodinách, vždy od 21:00. Zálohovat se bude datový disk, dále bude zvláštní záloha nastavena pro nastavení serverové stanice. Také je doporučeno zálohovat Active Directory po každé úpravě nastavení. Zálohy budou uloženy na samostatném pevném disku serverové stanice.

- **Nastavení zálohování**

Nejprve je nutno ve Správci serveru funkci Zálohování serveru nainstalovat. Toto provedeme v záložce Přidat role a funkce. Po instalaci se přes odkaz Správa dostaneme do nastavení zálohování. Následně zvolíme interval zálohování, disky, které se budou zálohovat a umístění, kde bude záloha uložena.

#### **4.5.6. Nastavení klientských počítačů**

Všechny počítače ve škole budou součástí domény zsHrabyne.cz a přihlašování bude pomocí síťových účtů. Na každé stanici bude nasdílena společná složka O:\, kde se budou ukládat materiály od učitelů a žáků, dále na všech učitelských stanicích bude nasdílena složka P:\, zde budou sdílet své materiály učitelé navzájem, a nakonec s každým uživatelským účtem bude spojena jeho síťová složka N:\, která bude rovněž nasdílena na stanici.

Každá klientská stanice obdrží údaje potřebné pro připojení k síti pomocí služby DHCP, jež bude nainstalovaná na serverové stanici.

Na každé stanici bude nahrazen výchozí administrátorský účet novým účtem s obdobnými právy, který se bude jmenovat zadmin a bude sloužit ke správě dané stanice. K tomuto účtu bude mít přístup správce sítě a ředitelka školy. Dále bude vytvořen univerzální lokální účet student, sloužící pro žáky nemající svůj síťový účet, a bude mít shodně omezená práva.

- **Postup registrace klientské stanice do domény**

Nejprve je nutné nastavit na klientské stanici získávání IP adresy automaticky pomocí DHCP. Toto provedeme v Ovládacích panelech v záložce Centrum síťových připojení a sdílení, kde vybere v pravém menu možnost Změnit nastavení adaptéru. Klikneme pravým tlačítkem myši na Ethernetový adaptér a zvolíme Vlastnosti, kde klikneme na Protokol IP verze 4 a opět zvolíme Vlastnosti. V následujícím okně zvolíme možnost Získávat IP adresu ze serveru DHCP automaticky a Získávat adresu DNS automaticky.

Následně na serveru v nabídce Uživatelé a počítače služby Active Directory přidáme novou stanici do organizační jednotky Stanice pomocí názvu příslušné stanice. Poté ve vlastnostech systému změníme název počítače a v části Je členem zvolíme možnost Domény a zadáme naši doménu zsHrabyne.

#### **4.6. Zabezpečení sítě**

Na všech klientských stanicích je v současné době nainstalován antivirus od společnosti ESET, ESET Endpoint Antivirus + File Security (v rámci ESET Secure Office). Tento antivirus má v sobě Antivirovou a Antispyware ochranu, která odstraňuje všechny typy hrozeb, včetně virů, rootkitů, červů a spyware. Součástí je také Firewall, bránící neautorizovanému přístupu do firemní sítě a chrání firemní data před zneužitím.

Síťový provoz mezi lokální sítí a světovou sítí je nutno zabezpečit Firewalllem. Tuto funkci zpravidla zastává zvláštní zařízení. Pokud se ovšem škola rozhodne zakoupit navrhovaný router TP-Link TL-R600VPN, nutnost koupě dalšího zařízení odpadá, jelikož tento router má Firewall již zabudovaný.

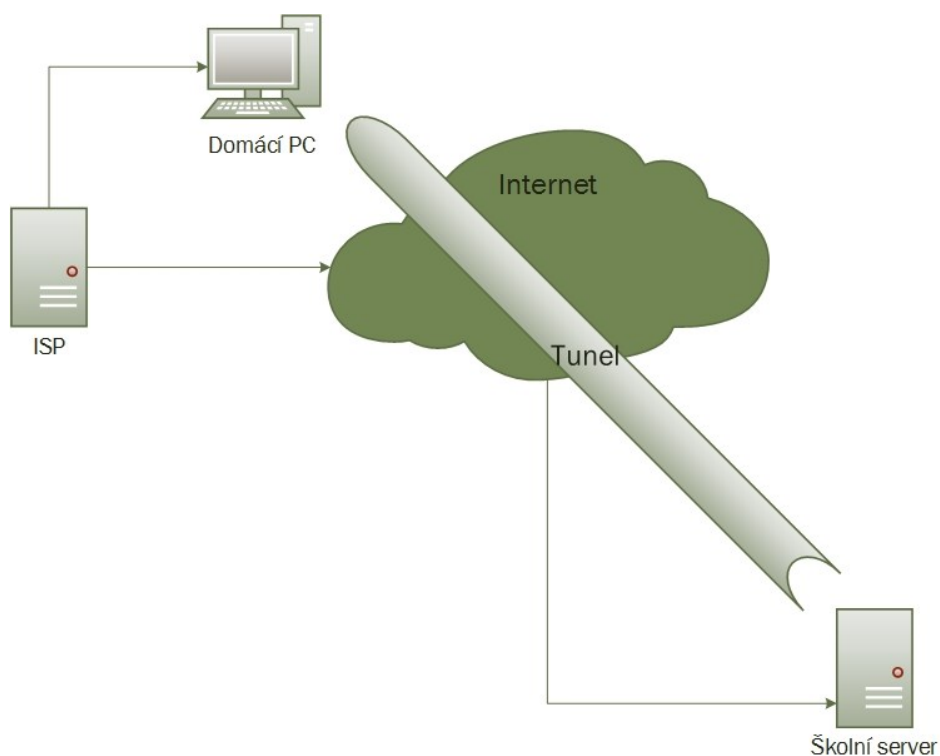
Kromě toho dokáže router automaticky rozpoznat DoS (Denial of Service) útoky, což jsou typy útoků na počítač nebo síť, které mají způsobit nedostupnost dané služby, typicky síťového připojení. Obvykle se provádí tak, že je cílový systém zahlcen ohromným množstvím nesmyslných dotazů. Mezi DoS útoky patří například Ping of Death, kdy útočník pošle abnormálně velký paket do sítě, kde dojde obvykle k selhání systému.

#### **4.7. Virtual Private Network**

VPN umožní, aby pedagogové nemuseli učební látku připravovat ve škole, anebo aby látku připravenou doma nemuseli nosit na přenosných paměťových médiích, které se mohou ztratit, bude k dispozici připojení ke školnímu serveru přes Virtuální Privátní Síť.

Učitelé budou moci své materiály připravit doma a přes VPN se připojit ke své složce, která se nachází na školním serveru a tam své materiály uložit. Ve škole potom z jakéhokoli počítače budou mít ke svým materiálům přístup.

Navrhovaný směrovač podporuje několik protokolů pro VPN připojení. Mezi tyto protokoly patří IPSec a PPTP. Tento router je dále vybaven vestavěnou hardwarovou technologií VPN, díky které může podporovat a spravovat až 20 LAN–LAN IPsec a 16 PPTP VPN připojení. Zásadou pokročilé technologie šifrování a ověřování představuje tento směrovač bezpečný způsob připojení do školní sítě.



Obrázek 4.3: Schéma VPN připojení. Zdroj: MS Visio, vlastní zpracování.

## 5. Zhodnocení navrhovaného řešení

Na základě požadavků vedení Základní školy v Hrabyni a jejich analýzy byl vytvořen návrh na implementaci serverové stanice do její stávající sítě. V návrhu byly zohledněny všechny aspekty, které ve škole jsou a které vedení školy požadovalo a všechny zadané požadavky se podařilo naplnit.

Stávající síť bude rozšířena o stanici se serverovým operačním systémem, na které budou nainstalovány veškeré výukové programy a bude tak vyřešen problém se stálou modernizací uživatelských stanic. Dále serverová stanice bude poskytovat služby DHCP, DNS, tiskového serveru a v neposlední řadě bude zastávat také roli doménového řadiče adresářové služby Active Directory, díky níž se zjednoduší sdílení souborů mezi učiteli a žáky a učitelé již nebudou muset své materiály nosit na paměťových zařízeních, ale budou k nim mít přístup ze kteréhokoliv počítače ve škole.

Na serverové stanici budou také zálohována veškerá data, záloha bude prováděna přímo na disku serveru. Vedení školy byla ovšem navržena možnost zvážení zakoupení extérního disku, aby při poškození disku, nebo serverové stanice nedošlo k nenávratné ztrátě veškerých dat.

Pokud se vedení školy rozhodne zakoupit navrhované aktivní prvky, budou učitelé moci využívat službu VPN, kterou navrhovaný router disponuje a budou moci přistupovat ke svým osobním složkám umístěným na školním serveru také z domova, ze svého soukromého počítače a dále v počítačové učebně vznikne prostor k případnému rozšíření počtu kabelově připojených stanic ke switchi o 8 kusů.

Vzhledem k absenci kritických aplikací běžících na serveru nebude zatím serverová stanice odolná vůči výpadkům elektrické energie, nicméně taktéž bylo vedení školy doporučeno zvážení zakoupení záložního zdroje UPS, který by při takovém výpadku zajistil korektní ukončení služeb a vypnutí stanice, aby nedošlo k poškození samotné stanice či pevných disků, na kterých budou uložena veškerá data.

Do budoucna by se mohlo využít dalších možností, které implementace serverové stanice nabízí a v tomto návrhu nejsou řešeny, například školní web by se mohl přesunout ze současného webhostingu na školní server, také by mohla být serverová stanice využita pro školní Moodle.

Pokud dojde ze strany vedení školy ke schválení tohoto návrhu a bude vyčleněn dostatek finančních prostředků, bude možné již v období letních prázdnin začít s implementací navrhovaného řešení. Implementace by měla být realizována autorem této práce ve spolupráci s firmou 24IT s.r.o, současného správce sítě a jež by po realizaci převzala správu také nad serverovou stanicí.

### 5.1. Finanční analýza navrhovaného řešení

	ks	Cena za ks	Cena celkem
<b>Router</b>			
TP-Link TL-R600VPN	1	2 489 Kč	2 489 Kč
<b>Switch</b>			
TP-Link TL-SG1024	1	3 075 Kč	3 075 Kč
<b>Server</b>			
HP ProLiant ML30 Gen9	1	21 990 Kč	21 990 Kč
<b>Software</b>			
Microsoft Windows Server 2012 R2 Standard	1	17 690 Kč	17 690 Kč
HP Microsoft Windows Server 2012 CAL 5 Device	5	3 355 Kč	16 755 Kč
<b>Kabeláž</b>			
UTP kabel cat.5e 1m	100	6 Kč	600 Kč
<b>Práce (odhadem)</b>			15 000 Kč
<b>Cena celkem</b>			77 599 Kč

Tabulka 5.1: Finanční analýza navrhovaného řešení.

Ceny v tabulce jsou včetně DPH a jsou platné k 28.4.2017, dle ceníku internetového obchodu [www.czc.cz](http://www.czc.cz), [www.tsbohemia.cz](http://www.tsbohemia.cz) a [www.bscom.cz](http://www.bscom.cz). Uvedené komponenty v tabulce jsou pouze navržené, jelikož škola je povinna dle zákona č. 137/2006 Sb. O veřejných zakázkách v aktuálním znění, jakožto státní příspěvková organizace, vypsát veřejné výběrové řízení na dodavatele veškerých komponent do nové sítě. Analýza je tudíž pouze orientační.

## 6. Závěr

Cíl této bakalářské práce byl rozdělen na dva podcíle. Prvním podcílem byl návrh implementace serverového řešení do školní sítě. Tento návrh byl vytvořen na základě požadavků a představ ze strany vedení školy o jeho fungování a druhým podcílem byla samotná realizace tohoto řešení.

V první části práce byly definovány teoretické poznatky týkající se počítačových sítí a serverového operačního systému. Hlavním bodem této práce byl síťový operační systém Windows Server 2012, jehož nejdůležitější funkce a role, které budou zahrnuty při realizaci návrhu do školního prostředí, byly podrobně specifikovány.

Následující část byla zaměřena na bližší seznámení s prostředím, ve kterém bude práce realizována, byla provedena analýza současného stavu a požadavků školy na nové fungování sítě.

V další kapitole této práce byl proveden návrh nové počítačové sítě, do níž byla zapojena také stanice se síťovým operačním systémem Windows Server 2012, proběhl výběr nových aktivních prvků sítě a konfigurace zmíněného síťového operačního systému tak, aby co nejpresněji následoval požadavky školy.

První stanovený podcíl této bakalářské práce, tzn. vytvoření návrhu inovace stávající sítě se zapojením serverové stanice, byl splněn. Druhý stanovený podcíl zatím splněn nebyl, neboť nejprve musí proběhnout výběrové řízení na nákup komponent a také by realizace mohla omezit výuku. Realizace navrhovaného řešení bude naplánována na období letních prázdnin, kdy už budou nakoupeny potřebné komponenty, a práce na realizaci nebude ve škole nikoho omezovat.



## Seznam použité literatury

HORÁK, Jaroslav a Milan KERŠLÁGER, 2011. *Počítačové sítě pro začínající správce*. 5., aktualiz. vyd. Brno: Computer Press. ISBN 978-80-251-3176-3.

KÁLLAY, Fedor a Peter Peniak, 2003. *Počítačové sítě LAN/MAN/WAN a jejich aplikace*. 2., aktualiz. vyd. Praha: Grada Publishing. ISBN 80-247-0545-1.

SOSINSKY, Barrie, 2010. *Mistrovství – počítačové sítě*. Brno: Computer Press. ISBN 978-80-251-3363-7.

STANEK, William R, 2015. *Microsoft Windows Server 2012: kapesní rádce administrátora*. Brno: Computer Press. ISBN 978-80-251-3817-5.

THOMAS, Thomas M, 2005. *Zabezpečení počítačových sítí bez předchozích znalostí*. Brno: CP Books. ISBN 80-251-0417-6.

TRULOVE, James, 2009. *Sítě LAN: hardware, instalace a zapojení*. Praha: Grada Publishing. ISBN 978-80-247-2098-2.

## Elektronické zdroje

Bscom, 2017. *Server HP ProLiant ML30 Gen9* [online]. Bscom. Poslední aktualizace 29. 4. 2017 [cit. 2017-04-29]. Dostupné z: [https://www.bscom.cz/server-hp-proliant-ml30-gen9-831068-425\\_d547315](https://www.bscom.cz/server-hp-proliant-ml30-gen9-831068-425_d547315).

KLIMŠA, Aleš, 2015. O nás. *ZŠ A MŠ HRABYNĚ* [online]. Aleš Klimša [cit. 2017-04-29]. Dostupné z: [http://hrabyne-skola.jupiter.savvy.cz/?page\\_id=304](http://hrabyne-skola.jupiter.savvy.cz/?page_id=304).

PETERKA, Jiří, 2012. *Počítačové sítě*. *eArchiv.cz* [online]. Jiří Peterka [cit. 2017-04-29]. Dostupné z: <http://www.earchiv.cz/1224/nahled.php3?l=2&me=1>.

TP-link, 2017. *Gigabitový širokopásmový VPN router SafeStream™ TL-R600VPN* [online]. TP-link Technologies Co. [cit. 2017-04-29]. Dostupné z: <http://cz.tp-link.com/products/details/TL-R600VPN.html>.

TP-link, 2017. *24portový gigabitový switch TL-SG1024* [online]. TP-link Technologies Co. [cit. 2017-04-29]. Dostupné z: [http://cz.tp-link.com/products/details/cat-42\\_TL-SG1024.html](http://cz.tp-link.com/products/details/cat-42_TL-SG1024.html).

## **Seznam zkratek**

ADDS – Active Directory Domain Services

CSMA/CD – Carrier Sense Multiple Access with Collision Detection

DHCP – Dynamic Host Configuration Protocol

DNS – Domain Name System

DoS – Denial of Service

GB – GigaByte

Gbps – Gigabits per second

HTTP – HyperText Transfer Protocol

IEEE – Institute of Electrical and Electronics Engineers

IP – Internet Protocol

IPsec – IP security

ISO – International Organization for Standardization

IT – Informační technologie

LAN – Local Area Network

MB – Mega Byte

Mbps – Megabits per second

PPTP – Point-to-Point Tunelling Protocol

TB – Tera Byte

TCP – Transmission Control Protocol

USB – Universal Serial Bus

VPN – Virtual Private Network

WLAN – Wireless Local Area Network

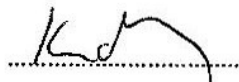
WWW – World Wide Web

## Prohlášení o využití výsledků bakalářské práce

Prohlašuji, že

- jsem byl seznámen s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. – autorský zákon, zejména § 35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo;
- beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB-TUO) má právo nevýdělečně, ke své vnitřní potřebě, bakalářskou práci užít (§ 35 odst. 3);
- souhlasím s tím, že bakalářská práce bude v elektronické podobě archivována v Ústřední knihovně VŠB-TUO a jeden výtisk bude uložen u vedoucího bakalářské práce. Souhlasím s tím, že bibliografické údaje o bakalářské práci budou zveřejněny v informačním systému VŠB-TUO;
- bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona;
- bylo sjednáno, že užít své dílo, bakalářskou práci, nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

V Ostravě dne 4.5.2017



Jan Kudela